

PARKER & McCONKIE  
JAMES W. McCONKIE (Bar # 2156)  
BRADLEY H. PARKER (Bar # 2519)  
Attorneys for Plaintiff  
5664 South Green Street  
Salt Lake City, Utah 84123  
Telephone: (801) 264-1950  
Facsimile (801)  
E-mail: [jwmcconkie@utahlawhelp.com](mailto:jwmcconkie@utahlawhelp.com)  
E-mail: [bparker@utahlawhelp.com](mailto:bparker@utahlawhelp.com)

COUNCIL ON AMERICAN-ISLAMIC  
RELATIONS  
LENA F. MASRI (DC: 1000019)\*  
GADEIR I. ABBAS (VA: 81161)\*  
Attorneys for Plaintiff  
National Litigation Director  
453 New Jersey Ave, SE  
Washington, DC 20003  
Phone: (202) 488-8787  
Facsimile: (202)  
E-mail: [lmarsri@cair.com](mailto:lmarsri@cair.com)  
E-mail: [gabbas@cair.com](mailto:gabbas@cair.com)

*\*Licensed in VA, not in Utah.  
A motion has been filed to admit  
Lena Marsi and Gadeir I. Abbas  
to appear in the matter.*

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF UTAH**

<b>YUSSUF AWADIR ABDI,</b>	)	
	)	
Plaintiff,	)	<b>Case No.</b>
	)	<b>Hon.</b>
v.	)	
	)	
<b>ANDREW MCCABE</b> , Acting Director of the	)	
Federal Bureau of Investigation, in his official	)	
capacity;	)	
	)	
<b>CHRISTOPHER M. PIEHOTA</b> , Director of the	)	
Terrorism Screening Center, in his official	)	
capacity;	)	
	)	

**HUBAN A. GOWADIA**, Acting Administrator, )  
Transportation Security Administration )  
(TSA), United States Department of )  
Homeland Security (DHS), in his official )  
capacity; )  
)

**KEVIN K. MCALEENAN**, Acting Commissioner )  
United States Customs and Border Protection; )  
in his official capacity, and, )  
)

**NICHOLAS J. RASMUSSEN**, Director of the )  
National Counterterrorism Center, in )  
his official capacity; )  
)

Defendants. )

---

**COMPLAINT FOR INJUNCTIVE AND DECLARATORY RELIEF**

Plaintiff, **Yusuf Awadir Abdi**, by and through his attorneys, CAIR National Legal Defense Fund, Inc. (“Council on American-Islamic Relations” or “CAIR”) and Parker & McConkie, states as follows:

**Introduction**

1. Through its No Fly List, the federal government is preventing an American citizen who is in Kenya now from returning to Utah where he lives.

2. To make matters worse, by preventing this citizen—who is a religious leader of his community—from flying back to the United States, the Defendants are preventing him from providing religious services to Muslims in Utah during the holy month of Ramadan.

3. These injuries are attributable to the Defendants systematically compiling a terrorist watch list, inventing consequences to inflict on listees, and disseminating this list to anyone willing to receive it.

4. It is why there is no exaggeration in stating that our federal government is imposing an injustice of historic proportions upon people such as Plaintiff Yusuf Awadir Abdi—who has not been arrested, charged, or convicted of any type of terrorism-related offense—as well as thousands of other Americans. Through extra-judicial and secret means, the federal government is ensnaring innocent Americans into an invisible web of consequences that are imposed indefinitely and without recourse because of the shockingly large federal terror watch list that now includes hundreds of thousands of individuals.

5. Indeed, many Americans, including children, end up on this secret federal terror watch list – which the Defendants have named the Terrorist Screening Database (“TSDB”) – based on mere guesses, hunches, and conjecture, and even simply based on matters of race, ethnicity, national origin, religion or the exercise of their constitutional rights.

6. These consequences include the inability to fly on airplanes, to go through security without having all screeners receive a message for the remainder of a listee’s life that he or she is a "known or suspected terrorist," to obtain licenses, to exercise their Second Amendment right to own a firearm, and to be free from the unimaginable indignity and real-life danger of having their own government communicate to hundreds of thousands of federal agents, private contractors, businesses, state and local police, the

captains of sea-faring vessels, and foreign governments all across the world that they are a violent menace.

7. And unfortunately, the federal government has designed its No Fly List to be accountability-free. Persons placed on the federal terror watch list have no means of challenging the constitutionality of their listing. Indeed, people on the federal terror watch lists only learn of their placement when they feel the web of consequences burdening their lives and aspirations, and they never learn the circumstances that led to their listing.

8. Media accounts have made clear that the secret federal terror watch list is the product of bigotry and misguided, counterproductive zeal. Americans are dumped onto the watch list without being charged, convicted, or in some stomach-churning cases, even subject to an ongoing investigation.

9. Instead, two leaked government documents and a governmental report, which include the March 2013 Watchlisting Guidance (Exhibit 2), the Directorate of Terrorist Identities (DTI): Strategic Accomplishments 2013 (Exhibit 3), and the Department of Justice's March 2014 Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist (Exhibit 4) reveal that the care the federal government takes in creating its federal terror watch list is void of proper processing, which in turn results in life-altering consequences that flow from these illegal actions.

10. In fact, upon information and belief, Dearborn, a city of less than 100,000 and a place Arab Americans and Muslim Americans have called home for generations, contains the second highest concentration of Americans on the federal government's watch list. Moreover, there have been more than 1.5 million nominations to the federal



terror watch list since 2009 and that, in 2013 for example, the Terrorist Screening Center converted 98.96 percent of those nominations into watch list placements.

11. Upon information and belief, evidence also shows that the federal government uses guilt-by-association presumptions to place family members and friends of listed persons on the watch list.

12. Moreover, travel to Muslim majority countries—travel that American Muslims are very likely to engage in—is also a basis for watch list placement.

13. In 2009, the federal government made 227,932 nominations to its federal terror watch list. In 2013, that number more than doubled at an alarming and dangerous rate to 468,749.

14. Recently, a federal court judge observed in *Gulet Mohamed v. Eric R. Holder, Jr.*, et al. (United States District Court, Eastern District of Virginia, Case No. 11-cv-00050 (2011)), that “[a] showing of past or ongoing unlawful conduct does not seem to be required,... But the Court has little, if any, ability to articulate what information is viewed by TSC as sufficiently ‘derogatory’ beyond the labels it has provided the Court. In sum, the No Fly List assumes that there are some American citizens who are simply too dangerous to be permitted to fly, no matter the level of pre-flight screening or on-flight surveillance and restraint, even though those citizens cannot be legally arrested, detained, or otherwise restricted in their movements or conduct.” *See* United States District Court, Eastern District of Virginia, Case No. 11-cv-00050 (2011); Dkt. 70 at 19; attached as Memorandum Opinion (Exhibit 1).

15. Moreover, the Court went on to find that “[i]nclusion on the No Fly List also labels an American citizen a disloyal American who is capable of, and disposed

toward committing, war crimes, and one can easily imagine the broad range of consequences that might be visited upon such a person if that stigmatizing designation were known by the general public... The process of nomination to the No Fly List is based on a suspected level of future dangerousness that is not necessarily related to any unlawful conduct.” *See* United States District Court, Eastern District of Virginia, Case No. 11-cv-00050 (2011); Dkt. 70 at 14, 17; attached as Memorandum Opinion (Exhibit 1).

### **Parties**

16. Plaintiff Yusuf Awadir Abdi is a United States Citizen and a Muslim residing in Salt Lake County, Utah.

17. Defendant Andrew McCabe is the Director of the Federal Bureau of Investigation (“FBI”). Defendant McCabe is responsible for the nominations of Plaintiff and other similarly situated American citizens to the federal terror watch list. Defendant McCabe is being sued in his official capacity, only.

18. Defendant Christopher M. Piehota is the Director of the Terrorist Screening Center (“TSC”). Defendant Piehota was appointed in April, 2013. Defendant Piehota develops and maintains the federal government’s consolidated Terrorism Screening Database (the “watch list”), and accepted the nominations of Plaintiff and other similarly situated American citizens to the federal terror watch list. Defendant Piehota also oversees the dissemination of the stigmatizing label attached to Plaintiff and other similarly situated American citizens of “known or suspected terrorists” to state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among

other official and private entities and individuals. Defendant Piehota is being sued in his official capacity, only.

19. Defendant Huban A. Gowadia is Acting Administrator of the Transportation Security Administration (“TSA”). Defendant Gowadia oversaw the dissemination of the stigmatizing label attached to Plaintiff and other similarly situated American citizens of “known or suspected terrorists” to state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals. Defendant Gowadia is being sued in his official capacity, only.

20. Defendant Kevin K. McCaleenan is Acting Commissioner of the National Counterterrorism Center (“NCTC”). Defendant McCaleena is responsible for the nominations that resulted in the placement of Plaintiff and other similarly situated American citizens on the federal terror watch list. Defendant McCaleenan is being sued in his official capacity, only.

### **Jurisdiction and Venue**

21. Under U.S. Const. Art. III §2, this Court has jurisdiction because the rights sought to be protected herein are secured by the United States Constitution. Jurisdiction is proper pursuant to 28 U.S.C. § 1331, *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971), *et seq.*, 5 U.S.C. § 702, 5 U.S.C. § 706, the United States Constitution, and federal common law.

22. This action seeks declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § § 2201-02, Rules 57 and 65 of the Federal Rules of Civil Procedure, and pursuant to the general, legal, and equitable powers of this Court.

23. A substantial part of the unlawful acts alleged herein were committed within the jurisdiction of the United States District Court for the District of Utah.

24. Venue is proper under 42 U.S.C. § 1391(e) as to all Defendants because Defendants are officers or employees of agencies of the United States sued in their official capacities and because this judicial district is where Plaintiff resides and where a substantial part of the events or omissions giving rise to the claims occurred.

### **Factual Background**

#### **Plaintiff Yussuf Awadir Abdi's Inability to Return to the United States**

25. Plaintiff Yussuf Awadir Abdi (hereinafter "Imam Abdi") is a Muslim religious leader and Imam of Madina Masjid Mosque in Salt Lake City, Utah.

26. Some time in 2014, the federal government placed Imam Abdi on the Selectee List component of the federal terror watch list, having secretly concluded that officials had a "reasonable suspicion" that Imam Abdi was "associated with terrorism." *See Exhibit 2.*

27. Imam Abdi knows that he was on the Selectee List because, for approximately the last three years, every time he travels by air, he is unable to check in to his flights online or at the kiosks stationed at the airports.

28. Rather, he is directed to check in manually with an airline representative in order to print his boarding pass.

29. The airline representative, after pulling up his name on the computer system, would contact the Department of Homeland Security in order to obtain clearance so that he could fly.

30. Once clearance from the Department of Homeland Security is obtained, the airline representative would then print his boarding pass, which would be stamped with the “SSSS” designation, indicating that he has been designated as a “known or suspected terrorist.”

31. Imam Abdi was then subjected to routine secondary inspections, prolonged searches and questioning every time he traveled by air.

32. Imam Abdi filed a redress request through DHS TRIP some time in 2016.

33. On May 22, 2017, Imam Abdi received a letter as described in paragraph 133 below and was assigned a Redress Control Number. While that letter contained many words, it provided no information—not notice of his placement nor some means by which to challenge his designation—about Imam Abdi’s status as a listee.

34. On June 14, 2017, Imam Abdi appeared at Jomo Kenyatta International Airport in Nairobi, Kenya to board a commercial flight back to his home in the United States.

35. Because his visa petitions that he filed for his wife and two of his children had just been approved, Imam Abdi had traveled to Kenya to bring his wife and five children with him to the United States. His remaining three children are United States Citizens.

36. Imam Abdi tried to check in at a kiosk stationed at the airport, however, he was directed to an airline representative to manually check him in for his flight.

37. Imam Abdi then presented himself at the Qatar Airlines ticket counter.

38. Although his wife and children were able to print their boarding passes, the Qatar Airlines representative told Imam Abdi that the United States would not allow him to board his flight in order to return to his home in the United States.

39. The following day, on June 15, 2017, Imam Abdi appeared at the United States Embassy in Nairobi, Kenya to obtain information as to why he was denied boarding and being prevented from returning to his home in the United States.

40. However, the United States Embassy did not provide him with any information.

41. Imam Abdi rescheduled his flight to the United States to leave later this evening on this date, June 16, 2017.

42. Upon information and belief, Imam Abdi was upgraded from the Selectee List to the No Fly List after he arrived in Kenya.

43. As a result, he was extrajudicially exiled from his country of citizenship, the United States.

44. Moreover, in the event that Imam Abdi is not removed from the No Fly List, he will be unable to board his flight rescheduled for tonight back home to the United States.

45. As a result of being denied boarding, Imam Abdi was unable to return home in time for the last ten nights of the holy month of Ramadan, the most important and blessed nights of Ramadan, when he is expected to lead prayers throughout each night at his mosque. The last ten nights of Ramadan began on the night of June 15, 2017.

46. Ramadan is a holy month of spirituality and devotion observed by Muslims worldwide, whereby Muslims fast from sunrise to sunset.

47. Moreover, Imam Abdi is designated to lead a group of Muslims to perform the Hajj, or religious pilgrimage in Saudi Arabia, which is scheduled to begin on August 30, 2017.

48. In the event Imam Abdi is not removed from the No Fly List, he will be unable to travel to Saudi Arabia to perform the Hajj, nor will he be able to lead the group that he is scheduled to lead.

49. At no time was Imam Abdi given notice of the factual basis for his placement on the federal terror watch list, and at no time was he offered a meaningful opportunity to contest his designation.

50. Moreover, at no time was Imam Abdi given notice of the deprivation of his liberty interests or violation of his constitutional rights.

51. Upon information and belief, Imam Abdi's nomination to and designation on the federal terror watch list was made based solely upon a hunch (based upon his race, ethnicity, national origin, religious affiliation, guilt-by-association, or First Amendment protected activities).

52. Upon information and belief, because Imam Abdi is included on the federal terror watch list, and specifically the No Fly List, Defendants disseminated and are continuing to disseminate his designation as a "known or suspected terrorist" to state and local authorities (including the local police officers above), foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, among other official and private entities and individuals.

53. Upon information and belief, because Imam Abdi is still included on the No Fly List, he remains unable to board a flight and return to his home in the United States.

### **The Federal Government's Terrorist Watch List**

54. In September, 2003, Attorney General John Ashcroft established the Terrorist Screening Center ("TSC") to consolidate the government's approach to terrorism screening. The TSC, which is administered by the FBI, develops and maintains the federal government's consolidated Terrorism Screening Database (the "watch list"). TSC's consolidated watch list is the federal government's master repository for suspected international and domestic terrorist records used for watch list related screening.

55. The watch list has two primary components: the Selectee List and the No Fly List. Persons on the Selectee List are systematically subject to extra screening at airports and land border crossings, and often find "SSSS" on their boarding passes printed by airline employees which is marked to indicate a passenger's watch list status to airline employees and screeners. Persons on the No Fly List, including Plaintiff, are prevented from boarding flights that fly into, out of, or even through United States airspace.

56. Defendant TSC disseminates records from its terrorist watch list to other government agencies that in turn use those records to identify suspected terrorists. For example, applicable TSC records are provided to TSA for use by airlines in pre-screening passengers and to CBP for use in screening travelers entering the United States by land.

57. Upon information and belief, Defendants disseminated the records of Plaintiff from their terrorist watch list to other government agencies, including Defendant



TSA for use by airlines in pre-screening Plaintiff, and Defendant CBP for use in screening Plaintiff upon entering the United States.

58. Upon information and belief, Defendants disseminated the records pertaining to Plaintiff from their terrorist watch list to foreign governments with the purpose and hope that those foreign governments will constrain the movement of Plaintiff in some manner.

59. Upon information and belief, Defendants' intention in disseminating watch list records, including those of Plaintiff and similarly situated American citizens, as widely as possible is to constrain their movements, not only within the United States, but abroad as well. For example, some countries detain individuals listed on the federal terror watch list who enter their borders, question those individuals at the behest of United States officials, or altogether prevent those individuals from even entering those countries.

60. Thus, while the TSC maintains and controls the database of suspected terrorists, it is the front-line agencies like the TSA that carry out the screening function. In the context of air travel, when individuals make airline reservations and check in at airports, the front-line screening agency, like TSA and CBP, conducts a name-based search of the individual, including that of Plaintiff, to determine whether he or she is on a watch list.

61. While agencies throughout the federal government utilize the federal terror watch list to conduct screening, listed persons are subject to a comprehensive portfolio of consequences that cover large aspects of their lives.

62. Indeed, Defendants disseminated the federal terror watch list to government authorities, private corporations and individuals with the purpose and hope that these entities and/or individuals will impose consequences on those individuals Defendants have listed, including Plaintiff.

63. Upon information and belief, the status of Plaintiff and similarly situated American citizens as known or suspected terrorists on the federal terror watch list diminishes and even imperils their ability to access the financial system.

64. Banks have closed the bank accounts of individuals listed on the federal terror watch list and financial companies have declined to allow some listed individuals to make wire transfers.

65. Moreover, upon information and belief, family-based immigration applications filed by Plaintiff and similarly situated American citizens are delayed indefinitely due to an "FBI name check" and not adjudicated, thereby denying Plaintiff and similarly situated American citizens of the rights that flow from citizenship, including the ability to sponsor for lawful permanent residency immediate relatives living abroad.

66. Among the entities and individuals that the federal government disseminates its federal terror watch list are state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among others.

67. In fact, in 2015, Defendant Piehota, Director of the Terrorist Screening Center, gave an exclusive interview to CNN and stated the following, in relevant part:

It's concerning that our partners don't use all of our data.  
We provide them with tools. We provide them with

support, and I would find it concerning that they don't use these tools to help screen for their own aviation security, maritime security, border screening, visas, things like that for travel.<sup>1</sup>

68. Defendant Piehota went on to state that the United States shares its federal terror watch list with the European Union, but that European Union countries do not systematically utilize it to identify suspected terrorists or screen migrants coming.

69. Upon information and belief, because the names of Plaintiff and similarly situated American citizens are included on the federal terror watch list, their names were disseminated to state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals.

70. Because the federal government disseminates its federal terror watch list to foreign governments, listed persons, including Plaintiff and similarly situated American citizens, are often not allowed to enter other nations. This is because the United States is telling other nations, without any modicum of due process, that thousands of its own citizens are “known or suspected terrorists.”

71. The federal government, through Defendants, disseminates its federal terror watch list to state and local police officers which allows those officers to query the names of persons, including Plaintiff, if for example, the listed individual is pulled over for routine traffic violations.

72. Disseminating the federal terror watch list to state and local police officers creates a dangerous situation insofar as the federal terror watch list effectively directs

---

<sup>1</sup> First on CNN: Top U.S. intel official: Europe not taking advantage of terror tracking tools, CNN, *available at*: <http://www.cnn.com/2016/04/07/politics/christopher-piehota-us-intel-europe-terror-tracking/>

state and local officers to treat thousands of Americans, including Plaintiff, charged or convicted with no crime yet listed as a “known or suspected terrorist” as extremely dangerous.

73. With the advent and deployment of automatic license plate readers by police departments across the country, local and state authorities have relied heavily upon a driver’s watch list status as the basis of a traffic stop, including Plaintiff and similarly situated American citizens.

74. Being on the federal terror watch list can prevent listed persons, including Plaintiff and similarly situated American citizens, from purchasing a gun. For example, New Jersey passed a law in 2013 that banned persons on the federal terror watch list from owning guns.

75. Accordingly, Plaintiff and similarly situated American citizens are unable to purchase guns in states that ban persons on the federal terror watch list from owning guns.

76. Because the federal government conducts a security risk assessment that includes querying the federal terror watch list prior to issuing a license to commercial drivers to transport hazardous materials, being on the federal terror watch list can prevent listed persons, including Plaintiff and similarly situated American citizens, from obtaining or renewing their Hazmat license.

77. Being on the federal terror watch list can also prevent listed persons, including Plaintiff and similarly situated American citizens, from accompanying minors or passengers with disabilities to their gate, from working at an airport, or working for an

airline insofar as listed persons are not allowed to enter so-called “sterile areas” of airports.

78. Being on the federal terror watch list can also result in the listing of the false stigmatizing label of “known or suspected” terrorist on the criminal records of Plaintiff and similarly situated American citizens, information that is publicly accessible to the general public.

79. Being on the federal terror watch list can also result in the denial or revocation of a Federal Aviation Administration (FAA) license of Plaintiff and similarly situated American citizens.

80. Although TSA, CBP, and other agencies may use the records provided by the TSC, it is the TSC that maintains and controls the database of suspected terrorists.

81. Two government entities are primarily responsible for “nominating” individuals for inclusion in the terrorist watch list—Defendants NCTC and FBI. The NCTC, which is managed by the Office of the Director of National Intelligence, relies on information from other federal departments and agencies when including alleged known or suspected international terrorists in its Terrorist Identities Datamart Environment (“TIDE”) database. The NCTC reviews TIDE entries and recommends specific entries to the TSC for inclusion in the watch list. TIDE is the main source of all international terrorist information included in the watch list.

82. Defendant FBI, in turn, nominates to the watch list individuals with what it characterizes as suspected ties to domestic terrorism.

83. Defendant TSC makes the final decision on whether a nominated individual meets the minimum requirements for inclusion into the watch list as a known

or suspected terrorist. TSC also decides which screening systems will receive the information about that individual.

84. Former Director of the Terrorism Screening Center Healy has testified that in evaluating whether an individual meets the criteria for inclusion on the consolidated watch list, the TSC determines whether the nominated individual is “reasonably suspected” of having possible links to terrorism. According to the TSC, “reasonable suspicion requires articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in and of or related to terrorism and terrorist activities.”

85. Defendants have not stated publicly what standards or criteria are applied to determine whether an American citizen on the consolidated watch list will be placed on the No Fly List, Selectee List (“SSSS”) or other list that is distributed to the TSA, CBP or other screening agencies.

86. The standards for watch list inclusion do not evince even internal logic. Defendants define a “suspected terrorist” as an “individual who is reasonably suspected to be, or have been, engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities based on articulable and reasonable suspicion.” In other words, Defendants place American citizens on the federal terror watch list based upon a “reasonable suspicion” that they are “reasonably suspected” of nefarious activities. This “reasonable suspicion” based on a “reasonable suspicion” standard does not even contain internal logic.

87. The federal government utilizes guilt-by-association as a basis for watch list inclusion. For example, the immediate relative of listed persons can be listed without any derogatory information—other than the bonds of family. Nonetheless, such designation suggests that the immediate relative is him or herself engaged in nefarious activities.

88. Being a known associate—a friend, colleague, fellow community member, etc.—of a listed individual can also provide a basis for watch list inclusion.

89. Even if an American citizen is acquitted of terrorism charges or those charges are otherwise dismissed, the federal government retains for itself the authority to continue to include them in the watch list.

90. For reasons unknown, Defendants also place what they call “non-investigatory subjects” on the federal terror watch list, American citizens that they have chosen not to investigate.

91. Under these practices and standards, the number of records in the consolidated watch list has swelled. Over 1.5 million nominations to the watch list have been submitted by federal agencies since fiscal 2009.

92. In 2013, Defendant TSC accepted 98.96 percent of all nominations made.

93. Because of these loose standards and practices, the federal terror watch list’s rate of growth has increased. In fiscal 2009, there were 227,932 nominations to the watch list. In fiscal 2013, there were 468,749 nominations.

94. Upon information and belief, in 2001, there were 16 people who the federal government systematically prevented from flying. In 2013, that number increased to 47,000.

95. Once an American citizen has been placed on the watch list, the individual remains on the list until the agency that supplied the initial information in support of the nomination determines the individual should be removed.

96. A 2007 GAO report found that TSC rejects only approximately one percent of all nominations to the watch list.<sup>2</sup> As such, the watch list is growing at a rate of approximately 20,000 entries per year.

97. At a March 10, 2010 Senate Homeland Security Committee hearing, Russel E. Travers, Deputy Director of the National Counterterrorism Center, stated that “[t]he entire federal government is leaning very far forward on putting people on list,” and that the watch list is “getting bigger, and it will get even bigger.”

98. The federal terror watch list disproportionately targets American Muslims.

99. Almost all publicly known instances of Americans being placed on the watch list regard Muslims or persons who could be mistaken for Muslims.

100. Defendants have utilized the watch list, not as a tool to enhance aviation and border security, but as a bludgeon to coerce American Muslims into becoming informants or forgoing the exercise of their rights, such as the right to have an attorney present during law enforcement questioning.

101. Public examples of this phenomenon abound. *See Latif v. Holder*, 2014 U.S. Dist. LEXIS 85450, \*19 (D. Or. June 24, 2014) (an FBI agent told Steven Washburn that he “would help remove Washburn's name from the No Fly List if he agreed to speak to the FBI”); *Id.* at \*21-22 (FBI agents told Ibraheim Mashal that “his name would be

---

<sup>2</sup> See United States Government Accountability Office Report to Congressional Requesters entitled *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110, October 2007, at 22.



removed from the No Fly List and he would receive compensation if he helped the FBI by serving as an informant.”): *Id* at \*22-23 (FBI agents offered Amir Meshal “the opportunity to serve as a government informant in exchange for assistance in removing his name from the No Fly List.”). *See also Fikre v. FBI*, 2014 U.S. Dist. LEXIS 73174 (D. Or. May 29, 2014) (Emirati officials told Yonas Fikre that he “could not travel to the United States by air because he is on the No Fly List” and an FBI agent told Fikre that “the FBI could take steps to remove [him] from the No Fly List if he agreed to be an informant.”); *Tanveer v. Holder, et. al.*, No. 13-cv-6951, Dkt. 15 (April 22, 2014) (Naveed Shinwari “declined to act as an informant for the Federal Bureau of Investigation and to spy on [his] own American Muslim communities and other innocent people.”).

102. Additionally, government records show that Dearborn, Michigan—which is 40 percent Arab—is disproportionately represented on the federal terror watch list. In fact, Dearborn is among the top five cities in the country, alongside Chicago, Houston, New York, and San Diego, represented on the federal terror watch list.

103. Due to Dearborn’s significant population of Muslims, it has earned a reputation as the “Muslim Capital of America.”

104. Defendants’ 2013 Watchlisting Guidance also indicates that “[t]ravel for no known lawful or legitimate purpose to a locus of terrorist activity” can be a basis for being listed. While a “locus of Terrorist Activity” is not defined by the document, upon information and belief, it likely includes any place where many Muslims reside.

105. The federal terror watch list's inclusion standards are so permissive and pliable and the selectee list's efficacy is at best fleetingly marginal that the inclusion standards themselves violate Plaintiff procedural and substantive due process.

106. The federal terror watch list diminishes, rather than enhances, our national security because the number of innocent Americans on the list is becoming so voluminous that the purpose of having a list is significantly undermined as all are being treated as the same.

107. The consequences of being on the federal terror watch list are meted out publicly. Members of the public can witness the extra screening to which individuals on the federal terror watch list are subject, oftentimes in front of family and colleagues, including being pulled out of their car at gunpoint, being ordered to leave their vehicle with their hands held above their head, among other stigmatizing measures.

108. In practice, frontline screeners disclose the status of individuals on the federal terror watch list to state and local authorities, as well as airline employees.

109. The operation of the federal terror watch list enlists air carriers to assist the federal government in tracking the passenger on the federal terror watch list.

110. Defendants apply the federal terror watch list against Muslim Americans in a manner that is different from how they use their list against people of other faith backgrounds.

111. Defendants use impermissible and inaccurate religious profiles in compiling the federal terror watch list.

112. Defendants who contributed to the placement of Plaintiff and similarly situated American citizens on the federal terror watch list knew that their actions violated clearly established federal law.

113. Defendants knew at the time they acted unlawfully that Supreme Court precedent required that, whenever a citizen is deprived of a liberty interest, the federal government must at least provide the deprived with some form of notice that a deprivation occurred.

**The Federal Government's Terrorist Watch List  
Is No More Effective Than a List of Randomly Selected Individuals**

114. Defendants' ability to watch list persons who pose a threat of terrorism, can be measured and described using a quantitative analysis based on factual allegations made in this Complaint as well as publicly available information describing the current operation of the federal terror watch list.

115. Upon information and belief, the federal government has placed approximately one million persons on the federal terror watch list over the last ten years.

116. Moreover, based on the University of Maryland's Global Terrorism Database, a project funded in part by the Department of Homeland Security, there have been less than 250 terrorist acts inside the United States over the last decade. These terrorist acts were perpetrated by less than 250 persons.

117. Only one of these perpetrators was designated on the federal terror watch list by the federal government prior to their criminal conduct. This single person designated on the federal terror watch list, however, was removed from the federal terror watch list prior to perpetrating the terrorist attack.

118. Upon information and belief, in order to designate a person on the federal terror watch list, the federal government must first have information about that person. Because the federal government does not possess information on every person in the world, existing law enforcement and intelligence practices produce a subset of persons who the federal government can then screen against the federal terror watch list's inclusion standards.

119. The precise size of this subset is unknown, however a survey of law enforcement and intelligence practices indicates that the size of this subset is greater than 50 million people.

120. Upon information and belief, the practices that produce this subset exclude some persons who do pose a threat of terrorism and include some persons who do not pose a threat of terrorism.

121. Upon further information and belief, the federal government does not screen the entire subset of people known to it. Moreover, Defendants do not make individual determinations as to whether each person about whom they know should be placed on the federal terror watch list.

122. In order to designate a person on the federal terror watch list, a federal government official must make a nomination and a TSC official must accept the nomination.

123. Upon information and belief, TSC officials accept nominations at a rate above 95 percent.

124. Based on the facts alleged in this Complaint and the publicly known processes of the federal terror watch list, a quantitative analysis can be constructed to measure and describe the performance of the federal terror watch list.

125. A quantitative analysis demonstrates that, in order to accomplish the federal terror watch list's stated objectives, Defendants must have at least some greater-than-random ability to identify future terrorists. This is due to the nature of the processes Defendants utilize to place persons on the federal terror watch list and the size of the population Defendants can—if they so choose—screen against the federal terror watch list's inclusion standards.

126. A quantitative analysis also demonstrates that Defendants' watch listing system would perform similarly if inclusion on the watch list was done via random selection instead of the existing inclusion standards Defendants utilize.

127. A quantitative analysis therefore indicates that Defendants have no ability to watch list persons whose placement on the watch list would further Defendants' stated objectives.

#### **Inadequacy of the DHS Traveler Redress Inquiry Program Process**

128. The government entities and individuals involved in the creation, maintenance, support, modification and enforcement of the federal terror watch list, including Defendants, have not provided travelers, including Plaintiff and similarly situated American citizens, with a fair and effective mechanism through which they can challenge the TSC's decision to place them on the terrorist watch list.

129. An individual, including Plaintiff and similarly situated American citizens, who has been prevented or hindered from travel by being placed on the federal terror

watch list has no clear avenue for redress, because no single government entity is responsible for removing an individual from the list. The TSC, which is administered by the FBI, does not accept redress inquiries from the public, nor does it directly provide final disposition letters to individuals on the selectee list or similarly situated American citizens, who have submitted redress inquiries. The NCTC which manages the TIDE list does not accept redress inquiries from the public.

130. Individuals who seek redress after having been included in the terrorist watch list must submit an inquiry through the DHS Traveler Redress Inquiry Program (“DHS TRIP”). DHS TRIP provides individuals with a “Redress Control Number.”

131. DHS TRIP is the only redress “process” available to individuals included on the terrorist watch list.

132. DHS TRIP submits traveler complaints to the TSC, which determines whether any action should be taken. The TSC has not provided any publicly available information about how it makes that decision. The TSC is the final arbiter of whether an individual’s name is retained on or removed from the watch list, including those of Plaintiff and similarly situated American citizens.

133. The TSC makes a determination regarding a particular individual’s status on the watch list, including Plaintiff and similarly situated American citizens, and DHS in turn responds to the individual with a standard form letter that neither confirms nor denies the existence of any terrorist watch list records relating to the individual. The letters do not set forth any basis for inclusion in a terrorist watch list, do not state whether the government has resolved the complaint at issue.

134. The government does not provide an American citizen with any opportunity to confront, or to rebut, the grounds for his or her possible inclusion on the watch list. As such, DHS TRIP offers no meaningful review of the watch list designation and in effect shields the TSC's actions with respect to the individual nominations or classes of nominations from meaningful review by any independent authority.

135. Moreover, the government's own internal audits of the system point to serious flaws. For example, a March 2008 DOJ Office of the Inspector General report entitled *Audit of the U.S. Department of Justice Terrorism Watchlist Nomination Processes* found significant problems with the nomination and removal process.

136. Thus, the only "process" available to such individuals is to submit their names and other identifying information to a government entity that has no authority to provide redress and to hope that an unspecified government agency corrects an error or changes its mind.

137. Plaintiff is a United States citizen.

138. Plaintiff has not been arrested, charged, nor convicted of a terrorism-related offense.

**COUNT I**  
**FAILURE TO PROVIDE POST-DEPRIVATION NOTICE AND HEARING IN**  
**VIOLATION OF THE FIFTH AMENDMENT RIGHT TO PROCEDURAL DUE**  
**PROCESS**  
**(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)**

139. The foregoing allegations are realleged and incorporated herein.

140. Plaintiff and other similarly situated American citizens learned that he was placed on the federal terror watch list subsequent to being added on the federal terror watch list and sought to challenge such placement.

141. Defendants' actions as described above in refusing to provide Plaintiff and other similarly situated American citizens with any notice at all of their placement which deprived Plaintiff and other similarly situated American citizens of constitutionally protected liberty interests.

142. Defendants' actions in nominating Plaintiff and other similarly situated American citizens to the federal terror watch list blatantly violate the requirement that "nominations' must not be solely based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities." 49 U.S.C. § 114(h)(3).

143. Plaintiff and other similarly situated American citizens have a liberty interest in traveling free from unreasonable burdens that are not reasonably tailored within, to, and from the United States, through land border crossings and over U.S. air space.

144. Plaintiff and other similarly situated American citizens have a right to be free from false government stigmatization as individuals who are "known or suspected to be" terrorists, or who are otherwise associated with terrorist activity, when such harm arises in conjunction with the additional consequences that follow from being listed as well as the deprivation of their right to travel on the same terms as other travelers and/or the deprivation of their liberty interest under the Fifth Amendment in travel free from unreasonable burdens.

145. Plaintiff and other similarly situated American citizens have a liberty interest in nonattainder (ie: the interest against being singled out for punishment without trial). Defendants' actions have singled out Plaintiff and others similarly situated for punishments that include, but are not limited to, inability to travel by air and



unreasonable burdens placed upon traveling by air to and from the United States, over U.S. air space and at land border crossings, and false association with a list of individuals suspected of terrorism.

146. Plaintiff and other similarly situated American citizens, having been burdened or prevented from boarding on commercial flights or entering the United States at land border crossings, having had their bank accounts closed, having been prevented from making wire transfers at financial institutions, having had their citizenship applications delayed indefinitely due to an “FBI name check,” having lost lucrative economic opportunities and suffering from other forms of financial harm, having been prevented from test driving or purchasing vehicles at a car dealership, and having sought to challenge their placement on the federal terror watch list, are entitled to a constitutionally adequate legal mechanism that affords them notice of the reasons and bases for their placement on the federal terror watch list and a meaningful opportunity to contest their continued inclusion on the federal terror watch list. Defendants have even failed to provide the most basic ingredient of due process, which is notice that the government has deprived a person of their protected rights.

147. Moreover, Defendants have officially imposed on Plaintiff and other similarly situated American citizens the stigmatizing label of “known or suspected terrorists” without a constitutionally adequate legal mechanism.

148. Further, Defendants disseminated the stigmatizing label attached to Plaintiff and other similarly situated American citizens of “known or suspected terrorists” to state and local authorities, foreign governments, private corporations, private

contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals.

149. By imposing on Plaintiff and other similarly situated American citizens the stigmatizing label of “known or suspected terrorists” and by failing to provide Plaintiff and others similarly situated with a constitutionally adequate legal mechanism, Defendants have deprived Plaintiff and other similarly situated American citizens of their protected liberty interests, including but not limited to their liberty interests in traveling, freedom from false stigmatization, and nonattainder, and thus violated the constitutional rights of Plaintiff and other similarly situated American citizens without affording them due process of law and will continue to do so into the future if Plaintiff and other similarly situated American citizens are not afforded the relief demanded below.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys’ fees incurred in this action.

**COUNT II**  
**DEPRIVATION OF PROTECTED LIBERTIES IN VIOLATION OF FIFTH**  
**AMENDMENT RIGHT TO SUBSTANTIVE DUE PROCESS**  
**(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)**

150. The foregoing allegations are realleged and incorporated herein.

151. Because Plaintiff and other similarly situated American citizens were listed by Defendants in a manner not narrowly tailored to a compelling interest, Defendants’ actions as described above in including Plaintiff and other similarly situated American citizens on a watch list that unreasonably burdens or prevents them from boarding commercial flights or entering the United States at land border crossings, are

arbitrary and capricious, lack even a rational relationship to any legitimate government interest, and have unduly deprived Plaintiff of constitutionally protected rights, including his liberty interests in travel, freedom from false stigmatization, and nonattainder.

152. Defendants' actions in nominating Plaintiff and other similarly situated American citizens to the No Fly List blatantly violate the requirement that "'nominations' must not be solely based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities." 49 U.S.C. § 114(h)(3).

153. By placing Plaintiff and other similarly situated American citizens on the federal terror watch list, Defendants have placed an undue burden on their fundamental right of movement.

154. By placing Plaintiff and other similarly situated American citizens on the federal terror watch list, Defendants have treated them like second-class citizens.

155. Defendants' watch list lacks a compelling interest insofar as their true purpose is to provide law enforcement with a tool to coerce American Muslims into becoming informants.

156. Defendants' watch list is also not narrowly tailored insofar as the federal terror watch list are entirely and demonstrably ineffectual and obvious alternatives exist.

157. Defendants' actions in placing Plaintiff and other similarly situated American citizens on the federal terror watch list, officially imposing on Plaintiff and other similarly situated American citizens the stigmatizing label of "known or suspected terrorists," and disseminating the stigmatizing label to state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private

entities and individuals, without a constitutionally adequate legal mechanism, are arbitrary and capricious, shock the conscience, violate the decencies of civilized conduct and are so brutal and offensive that they do not comport with the traditional ideas of fair play and decency.

158. Because Plaintiff and other similarly situated American citizens have not been charged with any crimes and are United States Citizens, Plaintiff challenges his placement and the placement of others similarly situated American citizens on the federal terror watch list on a broad, as-applied basis.

159. Plaintiff's substantive due process challenge is also facial, as there are no circumstances where his placement or the placement of others similarly situated on the federal terror watch list is narrowly tailored to achieve any compelling government interest.

160. Defendants have thus violated Plaintiff's constitutional rights and the constitutional rights of other similarly situated American citizens without affording them due process of law and will continue to do so into the future if Plaintiff and other similarly situated American citizens are not afforded the relief demanded below.

161. By placing Plaintiff and other similarly situated American citizens on the federal watch list, Defendants caused them an actual, imminent and irreparable injury that cannot be undone through monetary remedies.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

**COUNT III**

**UNLAWFUL AGENCY ACTION IN VIOLATION OF THE ADMINISTRATIVE  
PROCEDURE ACT, 5 U.S.C. §§ 702, 706  
(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)**

162. The foregoing allegations are realleged and incorporated herein.

163. Defendants' actions in placing Plaintiff and other similarly situated American citizens on the federal terror watch list, officially imposing on Plaintiff and other similarly situated American citizens the stigmatizing label of "known or suspected terrorists," and disseminating the stigmatizing label to state and local authorities, foreign governments, corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals, without a constitutionally adequate legal mechanism, were and are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and contrary to constitutional rights, power, privilege, or immunity, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

164. Defendants' actions in nominating Plaintiff and other similarly situated American citizens to the federal terror watch list blatantly violate the requirement that "nominations' must not be solely based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities." 49 U.S.C. § 114(h)(3).

165. Defendants' failure to provide Plaintiff and other similarly situated American citizens, who have been unreasonably burdened or denied boarding on commercial flights or entering the United States across the border and sought to challenge their placement on the federal terror watch list, with a constitutionally adequate mechanism that affords them notice of the reasons and bases for their placement on the

federal terror watch list and a meaningful opportunity to contest their continued inclusion on the federal terror watch list is arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and contrary to constitutional rights, power, privilege, or immunity, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

166. Because Plaintiff and other similarly situated American citizens do not present a security threat to commercial aviation, Defendants' actions as described above in including Plaintiff and other similarly situated American citizens on the federal terror watch list that unreasonably burdens or prevents them from boarding commercial flights or entering the United States across the border, are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and contrary to constitutional rights, power, privilege, or immunity, and should be set aside as unlawful pursuant to 5 U.S.C. § 706.

167. By placing Plaintiff and other similarly situated American citizens on the federal watch list, Defendants caused them an actual, imminent and irreparable injury that cannot be undone through monetary remedies.

168. Plaintiff and other similarly situated American citizens are not required to exhaust the DHS TRIP process, under the holding in *Darby v. Cisneros*, 509 U.S. 137 (1993). *See* United States District Court, Eastern District of Virginia, Case No. 11-cv-00050 (2011); Dkt. 70 at 22; attached as Memorandum Opinion (Exhibit 4).

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

**COUNT IV**

**VIOLATION OF THE FIFTH AMENDMENT  
TO THE UNITED STATES CONSTITUTION  
(Jurisdiction under 28 U.S.C. § 1331 and 5 U.S.C. § 702)  
(Equal Protection)**

169. The foregoing allegations are realleged and incorporated herein.

170. Defendants' actions in placing Plaintiff and other similarly situated American citizens on the federal terror watch list, officially imposing on Plaintiff and other similarly situated American citizens the stigmatizing label of "known or suspected terrorists," and disseminating the stigmatizing label to state and local authorities, foreign governments, private corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals, without a constitutionally adequate legal mechanism are discriminatory and constitute an action that targets religious conduct for distinctive treatment.

171. Defendants' actions in nominating Plaintiff and other similarly situated American citizens to the federal terror watch list blatantly violate the requirement that "'nominations' must not be solely based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities." 49 U.S.C. § 114(h)(3).

172. By placing Plaintiff and other similarly situated American citizens on the federal terror watch list, Defendants have treated Plaintiff and other similarly situated American citizens like second-class citizens.

173. Defendants' above-described actions were motivated by the religious status of Plaintiff and other similarly situated American citizens and on the basis of the

constitutionally-protected free exercise of religion of Plaintiff and other similarly situated American citizens.

174. Defendants' above-described actions have had a discriminatory effect upon and have disparately impacted Plaintiff and other similarly situated American citizens who are Muslim American travelers, and not travelers of other faiths.

175. Defendants' above-described actions, policies, course of conduct, or pattern of practice that mandate or permit the above-described treatment of Plaintiff and other similarly situated American citizens does not serve a compelling state interest or a legitimate or public purpose, nor are they the least restrictive means or narrowly tailored to achieve any such interest.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

**COUNT V**  
**VIOLATION OF THE UNITED STATES CONSTITUTION**  
**(Non-Delegation)**

176. The foregoing allegations are realleged and incorporated herein.

177. Congress has not provided the Executive Branch with intelligible principles from which the Executive can implement its watch list schemes regarding civil aviation and national security.

178. Congress has not directed the Executive Branch to create either a No Fly List or a Selectee List.



179. Congress has not authorized the Executive Branch to utilize the federal terror watch list to encourage financial institutions to close bank accounts or ban wire transfers, to encourage car dealerships to restrict test drives or purchases of vehicles, or state and local law enforcement to detain individuals based on their watch list status.

180. Congress has not authorized the Executive Branch to disseminate the terror watch list to local and state authorities, foreign countries, private corporations, private contractors, airlines, gun sellers, car dealerships, financial institutions, the captains of sea-faring vessels, among other official and private entities and individuals.

181. The Executive Branch's assignment of the watch listing function to TSC violates Congress' directive that TSA determine who belongs on federal terror watch lists and the consequences that flow from being on those lists.

182. Congress has not delegated to TSA the authority to create a process that can culminate in the removal of individuals from the TSDB.

183. In the alternative, Congress's delegation to TSA to create a redress process is defective because the Executive Branch has allocated watch list authority in a manner that prevents TSA from creating a redress process.

184. As a result, Defendants have illegally acted beyond their authority.

WHEREFORE, Plaintiff requests this Honorable Court grant declaratory and injunctive relief in the form described in the Prayer for Relief below, plus all such other relief this Court deems just and proper including costs and attorneys' fees incurred in this action.

### **Prayer for Relief**

WHEREFORE, Plaintiff respectfully requests:

1. A declaratory judgment that Defendants' policies, practices, and customs violate the Fifth Amendment to the United States Constitution and the Administrative Procedure Act;
2. An injunction that:
  - a. requires Defendants to remedy the constitutional and statutory violations identified above, including the removal of Plaintiff from any watch list or database that burdens or prevents him from flying or entering the United States across the border; and,
  - b. requires Defendants to provide individuals designated on the federal terror watch list with a legal mechanism that affords them notice of the reasons and bases for their placement on the federal terror watch list and a meaningful opportunity to contest their continued inclusion on the federal terror watch list;
3. A trial by jury;
4. An award of attorneys' fees, costs, and expenses of all litigation, pursuant to 28 U.S.C. § 2412; and,
5. Such other and further relief as the Court may deem just and proper.

Dated June 16, 2017

Respectfully submitted,

PARKER & McCONKIE

BY: /s/ James W. McConkie  
JAMES W. McCONKIE  
Utah State Bar # 2156  
Attorney For Plaintiff  
5664 South Green Street  
Salt Lake City, Utah 84123  
Phone: (801) 264-1950

PARKER & McCONKIE

BY: /s/ Bradley H. Parker  
BRADLEY H. PARKER  
Utah State Bar # 2519  
Attorney For Plaintiff  
5664 South Green Street  
Salt Lake City, Utah 84123  
Phone: (801) 264-1950

COUNCIL ON AMERICAN-  
ISLAMIC  
RELATIONS

BY: /s/ Lena Masri  
LENA F. MASRI (DC:  
1000019)\*  
Attorney for Plaintiff  
National Litigation Director  
453 New Jersey Ave, SE  
Washington, DC 20003  
Phone: (202) 488-8787

COUNCIL ON AMERICAN-  
ISLAMIC  
RELATIONS

BY: /s/ Gadeir Abbas  
GADEIR I. ABBAS (VA:  
81161)\*  
Attorney for Plaintiff  
National Litigation Director  
453 New Jersey Ave, SE

Washington, DC 20003  
Phone: (202) 488-8787

*\*Licensed in VA, not in Utah.  
A motion has been filed to  
admit  
Lena Masri and Gadeir I.  
Abbas  
to appear in the matter.*

*Counsel for Plaintiff*

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

GULET MOHAMED,	)	
	)	
Plaintiff,	)	
v.	)	No. 1:11-cv-50 (AJT/TRJ)
	)	
ERIC H. HOLDER, JR., <i>et al.</i> ,	)	
	)	
Defendants.	)	
_____	)	

**MEMORANDUM OPINION**

Plaintiff Gulet Mohamed has filed a three-count Third Amended Complaint based on his alleged placement on the No Fly List compiled by Defendant Terrorist Screening Center (the "TSC"). In Count I, Mohamed alleges that his constitutional right of reentry into the United States has been, and continues to be, infringed by his placement on the No Fly List. In Count II, Mohamed appeals, under the Administrative Procedure Act ("APA"), the TSC's decision to place him on the No Fly List, contending that the TSC's decision was arbitrary and capricious and contrary to law. In Count III, Mohamed alleges that he has been denied procedural due process in connection with his placement on the No Fly List. This matter is before the Court on Defendants' Motion to Dismiss Plaintiff's Third Amended Complaint [Doc. No. 58]. For the reasons set forth below, the Court concludes that, as applied to American citizens, the No Fly List raises substantial constitutional issues, and that the plaintiff has alleged facts sufficient to make plausible certain of his constitutional claims. The Motion will therefore be GRANTED in part and DENIED in part.



## **I. BACKGROUND**

### **A. Procedural History**

On January 18, 2011, Mohamed filed this action against Eric H. Holder, Jr., in his official capacity as Attorney General of the United States, Robert S. Mueller, III, in his official capacity as Director of the Federal Bureau of Investigation ("FBI"), and Timothy J. Healy, in his official capacity as Director of the TSC (collectively, the "Official Capacity Defendants"). Mohamed claims the Official Capacity Defendants violated his constitutional rights by placing him on the "No Fly List," the federal government's list of individuals on its terrorist watchlist who are prohibited from boarding commercial flights originating from or bound for destinations within the United States, and by preventing him from returning from Kuwait to the United States. Accompanying Mohamed's complaint was an application for emergency relief with respect to his alleged inability to return to the United States from Kuwait because of his placement on the No Fly List. After an initial hearing held on January 18, 2011, Mohamed's application for emergency relief became moot when he was permitted to return to the United States on January 21, 2011.

On May 20, 2011, Mohamed amended his complaint to add as defendants in their individual capacities "Unknown Agents," who he alleged tortured him in Kuwait, and "Unknown TSC Agents," who he alleged placed him on the No Fly List while he was abroad. In response, the defendants filed a motion to dismiss [Doc. No. 22], which the Court granted in part and denied in part on August 26, 2011 [Doc. Nos. 31-32]. In that Order, the Court dismissed those of Mohamed's claims against the Official Capacity Defendants that were based solely on his alleged inclusion in the Terrorist Screening Database ("TSDB") and on the No Fly List and transferred his remaining claims against the Official Capacity Defendants, as well as his claims

against the Unknown TSC agents, to the Court of Appeals for the Fourth Circuit pursuant to 49 U.S.C. § 46110, which gives the Courts of Appeals exclusive jurisdiction over challenges to certain orders of the Transportation Security Administration (“TSA”).<sup>1</sup> This Court retained jurisdiction over the remaining claims against the Unknown Agent Defendants. However, Mohamed failed to timely identify, join and serve those defendants and, on March 2, 2012, the Court dismissed the case as to those defendants pursuant to Fed. R. Civ. P. 4(m).

On May 28, 2013, the Court of Appeals entered an order vacating that portion of this Court’s Order dated August 26, 2011 that transferred certain claims to it and remanding the case to this Court for further proceedings, having concluded that it lacked exclusive jurisdiction over Mohamed’s claims pursuant to 49 U.S.C. § 46110. On August 29, 2013, Mohamed filed his Third Amended Complaint, which the defendants moved to dismiss on September 27, 2013. The Court held a hearing on the Motion to Dismiss on November 15, 2013, at which time it took the matter under advisement.

---

<sup>1</sup> 49 U.S.C. § 46110 provides in pertinent part:

(a) . . . [A] person disclosing a substantial interest in an order issued by the Secretary of Transportation . . . may apply for review of the order by filing a petition for review in the United States Court of Appeals for the District of Columbia Circuit or in the court of appeals of the United States for the circuit in which the person resides or has its principal place of business . . . .

(b) . . . When a petition is filed under subsection (a) of this section, the clerk of the court immediately shall send a copy of the petition to the Secretary, Under Secretary, or Administrator, as appropriate . . . .

(c) . . . When the petition is sent to the Secretary, Under Secretary, or Administrator, the court has exclusive jurisdiction to affirm, amend, modify, or set aside any part of the order and may order the Secretary, Under Secretary, or Administrator to conduct further proceedings.

**B. Factual Allegations**<sup>2</sup>

Briefly summarized, Mohamed alleges the following facts:

Mohamed, age 21, is a United States citizen and a resident of Alexandria, Virginia. Third Amend. Compl. ¶ 7. In March 2009, he “temporarily left the United States to learn Arabic and connect with members of his family living abroad.” *Id.* ¶ 37. Mohamed first studied Arabic for a few weeks in Yemen, but left “out of concern for his safety given the instability of the country” and traveled to Somalia, where he stayed with relatives for several months. *Id.* Around August 2009, Mohamed moved to Kuwait to continue his Arabic studies and stayed with an uncle. *Id.* Mohamed entered each country lawfully and maintained his lawful status during his travels abroad. *Id.*

On December 20, 2010, after having twice renewed his Kuwaiti visitor’s visa without incident, Mohamed went to again renew his visa at an airport in Kuwait. *Id.* ¶ 39. While he was at the airport, “two men in civilian clothes approached Mr. Mohamed, handcuffed him, blindfolded him, escorted him to a waiting SUV, and drove him to an undisclosed location approximately fifteen minutes from the airport.” *Id.* ¶ 40. Mohamed was held at that location for more than a week and “was repeatedly beaten and tortured by his interrogators,” one of whom spoke “perfect American English.” *Id.* ¶¶ 40-42.<sup>3</sup>

---

<sup>2</sup> The statements in this section are based on the allegations of the Third Amended Complaint, the declarations filed by the defendants with respect to the No Fly List and related programs, and those facts that currently appear undisputed based on the briefing pertaining to the Motion to Dismiss. The Court provides this statement of relevant facts solely for the purpose of ruling on the Motion to Dismiss. The Court also incorporates by reference its Memorandum Opinion dated August 26, 2011 [Doc. No. 31], which describes in detail the factual background of this case as well as the challenged government programs and procedures.

<sup>3</sup> Mohamed alleges the following details concerning his treatment while in detention:



On December 28, 2010, Mohamed's interrogators transferred him to a deportation facility, from which he was able to make contact with his family in the United States and retain a lawyer in the United States. *Id.* ¶¶ 44-45. Kuwaiti officials told Mohamed's family that he was being held at the behest of the United States government. *Id.* ¶ 46. Further, the Kuwaiti officials attempted to deport Mohamed but were unable to do so because the United States had placed him on the No Fly List. *Id.* While at the deportation facility, Mohamed received two visits from FBI agents, on December 28, 2010 and January 12, 2011. *Id.* ¶¶ 47-48. During those visits, the FBI agents told him that "they could expeditiously procure his release from detention if Mr. Mohamed spoke to them," and that "he would remain in detention indefinitely if he did not speak to them." *Id.* ¶ 47. The agents questioned Mohamed for hours, even after he repeatedly asked them to stop, and they threatened future interrogations and criminal charges. *Id.* ¶ 48. On January 16, 2011, Mohamed's family purchased a ticket for him to return to the United States at the suggestion of Kuwaiti officials, who delivered the ticket to Mohamed and transported him to the airport, where he was denied boarding.<sup>4</sup> *Id.* ¶ 49.

On January 18, 2011, Mohamed, through his American lawyer, filed this action, together with a request for emergency relief to obtain Mohamed's return to the United States. The Court

---

Mr. Mohamed's interrogators struck him in the face with their hands regularly and in Mr. Mohamed's estimate more than a hundred times. The interrogators whipped his feet and other parts of his body with sticks. Mr. Mohamed was forced by his interrogators to stand for prolonged periods of time. At one point, the interrogators threatened to run currents of electricity through Mr. Mohamed's genitals. In another instance, Mr. Mohamed's arms were tied to a ceiling beam and left in that position until he lost consciousness . . . . Mr. Mohamed remained blindfolded and handcuffed most of the time.

Third Amend. Compl. ¶¶ 40-41.

<sup>4</sup> Based on the other facts alleged, the Third Amended Complaint's listing of the date as January 16, 2010 is clearly an error.

held a hearing on the emergency request that same day but continued the hearing to January 20, 2011 at the defendants' request and based on their representations concerning their efforts to place Mohamed on a flight back to the United States. On January 20, 2011, the defendants advised the Court that arrangements had been made for Mohamed to return to the United States that day, and on January 21, 2011, Mohamed arrived in the United States by commercial airliner without escort or restraints and without incident. *See id.* ¶ 50. Since his arrival in the United States, Mohamed has not been criminally charged or otherwise detained.

Mohamed alleges that the FBI "does not limit its nominations [for inclusion on its terrorist watchlist] to persons it believes pose a threat to commercial aircraft . . . [but] also nominates individuals it considers as a broader threat to domestic or international security." *Id.* ¶ 22. Further, Mohamed alleges that "Defendants placed Mr. Mohamed on its No Fly List while he was abroad in order to pressure him to forgo his right to counsel, submit to invasive questioning, and become an informant for the FBI upon returning to the United States." *Id.* ¶ 2. Finally, Mohamed alleges that this improper use of the No Fly List extends beyond his own experience and that the FBI has repeatedly used the No Fly List "not just to protect commercial aircraft, but rather to coerce a specific subset of Americans—Muslim citizens—to forgo their rights, obstruct their ability to move freely, and otherwise give Defendants' agents leverage over listed persons." *Id.* ¶ 3.

Mohamed claims that his placement on the No Fly List constitutes: (1) a violation of his right as a U.S. citizen to reside in the United States and reenter it from abroad (Count I); (2) unlawful agency action that violates his Fourteenth Amendment right to return to the United States and his Fifth Amendment liberty interests "in traveling by air and being free from false governmental stigmatization as a terrorist" (Count II); and (3) a violation of his right to

procedural due process, including his right to pre- or post-deprivation notice and a hearing (Count III).

**C. The Terrorist Screening Center and Terrorist Screening Database**

Following the attacks of September 11, 2001, Congress and the President mandated that federal executive departments and agencies share terrorism information with those in the counterterrorism community responsible for national security. Piehota Decl., ¶ 4.<sup>5</sup> Specifically, Congress directed that the TSA, “in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers (A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and (B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual.” 49 U.S.C. § 114(h)(3).

On September 16, 2003, through Homeland Security Presidential Directive (“HSPD”)-6, President Bush sought to consolidate the government’s approach to terrorist prevention activities. Toward that end, the Attorney General, pursuant to HSPD-6, established the TSC as a multi-

---

<sup>5</sup> In support of their Motion to Dismiss, the defendants have submitted the declarations of Mark Giuliano, Laura Lynch, and Christopher Piehota, which speak to the specific programs, agencies and other matters referenced and alleged in the Third Amended Complaint. The Court has considered these declarations in connection with the defendants’ jurisdictional challenges based on lack of standing, ripeness and exhaustion of remedies as well as their motion to dismiss the Third Amended Complaint on the grounds that it fails to state claims as a matter of law. *See Velasco v. Gov’t of Indonesia*, 370 F.3d 392, 398 (4th Cir. 2004) (matters outside the pleadings may be considered in connection with jurisdictional challenges); *see also Katyle v. Penn Nat. Gaming, Inc.*, 637 F.3d 462, 466 (4th Cir. 2011) (on a motion to dismiss, the court may consider documents referenced by the complaint and matters of which it may take judicial notice).

agency center for coordinating information pertaining to terrorist activity.<sup>6</sup> *Id.* ¶ 2. HSPD-6 also directed the creation of the Terrorist Screening Database (“TSDB”) as the government’s consolidated terrorist watchlist maintained by the TSC. *Id.* ¶ 6. In creating the TSDB, the government consolidated as many as twelve preexisting watchlists, including the No Fly List. *Id.* ¶¶ 5-6.<sup>7</sup>

The TSC determines whether to place individuals in the TSDB based on “nominations” received from the National Counterterrorism Center (“NCTC”) and the FBI. *Id.* ¶¶ 8-10. The TSC places a nominated individual in the TSDB if the nomination is supported by “minimum substantive derogatory criteria.” *Id.* ¶ 10. Whether an individual satisfies the substantive derogatory criteria necessary to be placed in the TSDB is “generally based on whether there is reasonable suspicion to believe that a person is a known or suspected terrorist.” *Id.* ¶ 12. In order to meet this standard, “the nominator, based on the totality of the circumstances, must rely upon ‘articulable’ intelligence or information which, taken together with rational inferences from those facts, creates a reasonable suspicion that the individual is a known or suspected terrorist.”<sup>8</sup> *Id.* By contrast, “[m]ere guesses or ‘hunches,’ or the reporting of suspicious activity alone are not enough to constitute a reasonable suspicion and are not sufficient bases to watchlist an

---

<sup>6</sup> The TSC receives support from, *inter alia*, the Department of Justice, the Department of Homeland Security, the Department of State, and the Office of the Director of National Intelligence, and is staffed by officials from those agencies and also the FBI, the TSA, and U.S. Customs and Border Protection. Pichota Decl., ¶ 2.

<sup>7</sup> The No Fly List was originally maintained by the TSA, which was formerly within the Department of Transportation and is now part of Department of Homeland Security. Pichota Decl., ¶ 5.

<sup>8</sup> The TSDB itself does not contain any “derogatory intelligence information” but is limited to “sensitive but unclassified terrorist identity information consisting of biographic identifying information such as name or date of birth or biometric information such as photographs, iris scans, and fingerprints.” Pichota Decl., ¶ 6.

individual.” *Id.* Likewise, “nominations must not be solely based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities.” *Id.* “TSC personnel” make the decision of whether to place an individual in the TSDB, and “TSA employees assigned to and stationed at the TSC serve as subject matter experts regarding those individuals nominated to the No Fly and Selectee Lists.” *Id.* ¶¶ 11-13.

The No Fly List is a subset of individuals included in the TSDB and is defined by the Department of Homeland Security (“DHS”) as “a list of individuals who are prohibited from boarding an aircraft.” *Id.* ¶ 16. The Selectee List, another subset of the TSDB, is “a list of individuals who must undergo additional security screening before being permitted to board an aircraft.” *Id.* In order for the TSC to place an individual on the No Fly or Selectee List, his nomination must meet unspecified “additional derogatory requirements” in addition to the “minimum substantive derogatory criteria” required for placement in the TSDB. *Id.* ¶ 10.

Through its Secure Flight Program, the TSA receives information on passengers from airlines and compares it to information contained in government watchlists, including the No Fly and Selectee Lists. Lynch Decl., n.1. An airline cannot issue a boarding pass until it receives permission from the TSA. In addition, “[t]he TSC, through the TSDB, makes terrorist identity information accessible to various screening agencies and law enforcement entities by the regular export of updated subsets of TSBD data. For example, the No Fly and Selectee Lists are available for passenger and employee screening.” Pichota Decl., ¶ 15.

The TSC and the other agencies involved operate under a directive to maintain “thorough, accurate, and current information within the TSDB.” *Id.* ¶ 19. To meet that directive, “several quality control measures are continuously applied by nominating agencies, the TSC, and NCTC,” including “periodic reviews and audits to guarantee the integrity of the information

relied upon for the maintenance of TSDB records, and an ongoing responsibility upon the nominating agencies to notify NCTC and TSC of any changes that could affect the validity or reliability of that information.” *Id.* That review process does not include any disclosure to the individual involved or any judicial oversight or review before a person is included in the TSDB or placed on the No Fly List.

Congress has mandated that DHS “shall establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat under the regimes utilized by the Transportation Security Administration, United States Customs and Border Protection, or any other office or component of the Department of Homeland Security.” 49 U.S. § 44926(a). DHS is also required to “establish a procedure to enable airline passengers, who are delayed or prohibited from boarding a flight because the advanced passenger prescreening system determined that they might pose a security threat, to appeal such determination and correct information contained in the system.” 49 U.S. 44903(j)(2)(C)(iii).

In response to these congressional mandates, the TSA has established a procedure called DHS Traveler Redress Inquiry Program (“DHS TRIP”), through which the government provides redress to travelers who have been referred for additional screening or delayed or denied airline boarding for any reason, including because of their alleged placement on the No Fly List. Piehota Decl., ¶ 26. To initiate the review process, the traveler must first submit a traveler inquiry form to DHS. Lynch Decl., ¶ 5. When a traveler’s inquiry seems related to the TSDB, it is referred to the TSC, which determines whether the traveler is an exact match to an individual listed in the TSDB. Piehota Decl., ¶ 29. If there is a match, the TSC works in collaboration with the agency that nominated the individual to determine whether the individual’s current status is

appropriate. *Id.* ¶¶ 29-31. After its review, the TSC notifies the TSA, which sends a determination letter to the traveler. Lynch Decl., ¶ 10. The determination letter does not reveal whether the individual is, or ever was, on the No Fly List, or the reasons for his status. Piehota Decl., ¶ 32. The DHS TRIP letter advises, however, that the inquiring traveler can seek judicial review of the TSA's actions in the United States Court of Appeals pursuant to 49 U.S.C. § 46110 and may also indicate that the traveler can pursue an administrative appeal with the TSA. Lynch Decl., ¶ 11.

## **II. ANALYSIS**

### **A. Interests Implicated by the No Fly List, as Applied to American Citizens**

It is among the most compelling of governmental duties to protect our country from its enemies, foreign and domestic. Today, we are at war with those who would, if possible, use a commercial aircraft as an instrument of mass murder. There can be no doubt that the government has the right and obligation to identify, investigate and stop those who present such a threat; and for that purpose, the government must collect and act on intelligence information concerning possible terrorists, while protecting its sources and methods. It is a task of the highest national priority, performed by dedicated Americans whose mission is to protect this country and its citizens. It is because the stakes are so high and the consequences of a lapse in security so potentially catastrophic that the central issue presented in this case—how to adequately protect our population from terrorist threats while remaining faithful to the basic liberties that define the society we seek to preserve—is so difficult. For this reason, the constitutional issues pertaining to the No Fly List cannot be responsibly addressed without an informed, fact-based record that allows an assessment of the unavoidable trade-off between



security and personal liberties and whether the No Fly List, and its associated procedures and uses, strikes the appropriate balance between the two.

At first blush, it may seem a small intrusion upon the fabric of our freedoms to eliminate the ability of a relatively small number of American citizens to fly on commercial airlines in order to avert a possible catastrophic air disaster, such as occurred over Lockerby, Scotland in 1988, or nearly occurred through the efforts of the “Shoe Bomber” in 2001<sup>9</sup> or the “Christmas Day bomber” in 2009,<sup>10</sup> particularly if there is a process in place dedicated to limiting that restriction to those reasonably suspected to be terrorists. *See* Piehota Decl., ¶ 12. We were recently reminded by the Boston Marathon bombings that there are, indeed, those living among us who seek to indiscriminately kill on American soil. And the No Fly List is designed to protect a particularly vulnerable population—those who fly on commercial airlines. *See, e.g., United States v. Hartwell*, 436 F.3d 174, 179 (3d Cir. 2006) (“[T]here can be no doubt that preventing terrorist attacks on airplanes is of paramount importance.”). Extended analysis is not required, however, to understand that the No Fly List implicates some of our basic freedoms and liberties as well as the question of whether we will embrace those basic freedoms when it is most difficult.

The impact on a citizen who cannot use a commercial aircraft is profound. He is restricted in his practical ability to travel substantial distances within a short period of time, and

---

<sup>9</sup> On December 22, 2001, Richard Reid, the “Shoe Bomber,” attempted to detonate explosives hidden in his shoes during a flight from Paris to Miami. He was sentenced to life in prison.

<sup>10</sup> On December 25, 2009, Umar Farouk Abdulmutallab, the “Christmas Day bomber,” attempted to detonate, in flight, explosives concealed in his underwear. He was convicted of, among other charges, attempted murder and conspiracy to commit an act of terrorism transcending national boundaries, and was sentenced to life in prison. Mohamed alleges that following this event, the defendants “dramatically expanded the watch list as a whole and the No Fly List in particular.” Third Amend. Compl. ¶ 30.



the inability to fly to a significant extent defines the geographical area in which he may live his life. As a practical matter, an affected person is restricted in his ability to visit family and friends located in relatively distant areas of the country or abroad, which through flight can be reached within a matter of hours but would otherwise take days, if not weeks, to access. *See Latif v. Holder*, No. 3:10-cv-750, 2013 WL 4592515, at \*8 (D. Or. Aug. 28, 2013) (noting that flight is often the only feasible form of international travel); *Ibrahim v. Dep't of Homeland Sec.*, No. C 06-00545 WHA, 2012 WL 6652362, at \*7 (N.D. Cal. Dec. 20, 2012) (same). An inability to travel by air also restricts one's ability to associate more generally, and effectively limits educational, employment and professional opportunities. It is difficult to think of many job categories of any substance where an inability to fly would not affect the prospects for employment or advancement; one need only reflect on how an employer would view the desirability of an employee who could not travel by air. An inability to fly likewise affects the possibility of recreational and religious travel, given the time periods usually available to people, particularly those who are employed.<sup>11</sup>

---

<sup>11</sup> The extent to which the No Fly List is "exported" to agencies and entities other than the TSA is not clear from the present record. However, it does appear that such information has a much broader distribution than merely to the TSA, extending to other law enforcement and passenger screening agencies as well as for use in employment screening. *See* Piehota Decl., ¶ 15 ("The TSC, through the TSDB, makes terrorist identity information accessible to various screening agencies and law enforcement entities by the regular export of updated subsets of TSDB data. For example, the No Fly and Selectee Lists are subsets of TSDB information that are available for passenger and employee screening."). The court in *Latif* observed that the TSC shares watchlist information with twenty-two foreign governments and that United States Customs and Border Protection makes recommendations to ship captains as to whether a passenger poses a risk to transportation security. *See Latif*, 2013 WL 4592515, at \*9. This type of distribution, of course, only compounds the restrictions on travel and other effects placement in the TSDB has on an American citizen.

Inclusion on the No Fly List also labels an American citizen a disloyal American who is capable of, and disposed toward committing, war crimes, and one can easily imagine the broad range of consequences that might be visited upon such a person if that stigmatizing designation were known by the general public. In effect, placement on the No Fly List is life defining and life restricting across a broad range of constitutionally protected activities and aspirations; and a No Fly List designation transforms a person into a second class citizen, or worse. The issue, then, is whether and under what circumstances the government should have the ability to impose such a disability on an American citizen, who should make any such decision, according to what process, and by what standard of proof.

The War on Terrorism in which the United States is currently engaged is not the first time the judicial branch has had occasion to consider these national security issues. During the Cold War, with its threat of unbridled nuclear war, the courts considered the constitutionality of laws limiting the issuance of passports in order to restrict the travel of American citizens suspected of subversive, Communist activities that, as reflected in congressional findings,<sup>12</sup> were perceived as raising public safety and national security concerns comparable to those associated with the

---

<sup>12</sup> In support of the Subversive Activities Act of 1950, Congress found that there “exists a world Communist movement . . . whose purpose it is, by treachery, deceit, infiltration, . . . espionage, sabotage, terrorism, and any other means deemed necessary, to establish a communist totalitarian directorship in the countries throughout the world through the medium of a world-wide Communist organization.” *Aptheker v. Sec’y of State*, 378 U.S. 500, 508 n.8 (1964). Congress further found that the Communist organization in the United States and the world Communist movement presented a danger to the security of the United States that required legislative action. With respect to the restrictions of Section 6 of the Act, pertaining to the issuance of passports, Congress more specifically found that “[d]ue to the nature and scope of the world Communist movement, with the existence of affiliated constituent elements working toward common objectives in various countries of the world, travel of Communist members, representatives, and agents from country to country facilitates communication and is a prerequisite for the carrying on of activities to further the purposes of the Communist movement.” *Id.*

threats of terrorism today. In a series of cases, the federal courts, including the United States Supreme Court, addressed the constitutional limits on the government's reach over a citizen's freedom of movement. For example, in *Kent v. Dulles*, 357 U.S. 116 (1958),<sup>13</sup> the Supreme Court considered the right to travel and the protections it enjoyed from restrictions in the name of national security:

The right to travel is a part of the 'liberty' of which the citizen cannot be deprived without the due process of law under the Fifth Amendment . . . . In Anglo-Saxon law that right was emerging at least as early as the Magna Carta. Chafee, *Three Human Rights in the Constitution of 1787* (1956), 171-181, 187 *et seq.*, shows how deeply engrained in our history this freedom of movement is. Freedom of movement across frontiers in either direction, and inside frontiers as well, was a part of our heritage. Travel abroad, like travel within the country, may be necessary for a livelihood. It may be as close to the heart of the individual as the choice of what he eats, or wears, or reads. Freedom of movement is basic to our scheme of values. 'Our nation,' wrote Chaffee, 'has thrived on the principle that, outside areas of plainly harmful conduct, every American is left to shape his own life as he thinks best, do what he pleases, go where he pleases.'

*Id.* at 125-26 (some citations omitted). Observing that the government has been allowed in times of war to exclude citizens from their homes and restrict their freedom of movement only upon a showing of "the gravest imminent danger to the public safety," the *Kent* Court reaffirmed that:

[T]he right of exit [from the United States] is a personal right included within the word 'liberty' as used in the Fifth Amendment. If that 'liberty' is to be regulated, it must be pursuant to the lawmaking functions of the Congress. And if that power is delegated, the standards must be adequate to pass scrutiny by the accepted tests. Where activities or enjoyment, natural and often necessary to the well-being of an American citizen, such as travel, are involved, we will construe narrowly all delegated powers that curtail or dilute them.

*Id.* at 128-29 (internal citations omitted). In summary, the Court emphasized that in dealing with restrictions on travel, such as those imposed in that case, "[w]e deal with beliefs, with

---

<sup>13</sup> In *Kent*, the Court considered a challenge to regulations promulgated by the Secretary of State that prohibited the issuance of passports to members of the Communist Party and individuals engaged in activities in support of the Communist movement. The Court held that the Secretary of State lacked the authority to promulgate the regulations and therefore did not reach the question of whether the regulations would be constitutional if authorized.

associations, with ideological matters. We must remember that we are dealing with citizens who have neither been accused of crimes nor found guilty.” *Id.* at 130.

The Court revisited the constitutionality of statutory restrictions on the right to travel in *Aptheker v. Secretary State*, 378 U.S. 500 (1964). There, the Court reviewed the constitutionality of Section 6 of the Subversive Activities Control Act of 1950, which made it unlawful for any member of a registered Communist organization with knowledge or notice of the registration to apply for or use a U.S. passport. The Court recognized that “freedom of travel is a constitutional liberty closely related to rights of speech and association,” and in declaring Section 6 unconstitutional, reaffirmed that “a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.” *Id.* at 508, 517 (quoting *NAACP v. Alabama*, 377 U.S. 288, 307 (1964)). The Court recognized that the application of these principles required it to consider the congressional purpose underlying the restrictions on the right to travel:

The Government emphasizes that the legislation in question flows, as the statute itself declares, from the congressional desire to protect our national security. That Congress under the Constitution has power to safeguard our Nation’s security is obvious and unarguable. As we said in [*Kennedy v. Mendoza-Martinez*, 372 U.S. 144, 159-60 (1963)], ‘while the Constitution protects against invasions of individual rights, it is not a suicide pact.’ At the same time the Constitution requires that the powers of government must be so exercised as not, in attaining a permissible end, unduly to infringe a constitutionally protected freedom.

*Id.* at 509 (some internal citations and quotation marks omitted).

The Court in *Aptheker* concluded:

[Section 6] sweeps too widely and too indiscriminately across the liberty guaranteed in the Fifth Amendment. The prohibition against travel is supported only by a tenuous relationship between the bare fact of organizational membership and the activity Congress sought to proscribe. The broad and enveloping prohibition indiscriminately

excludes plainly relevant considerations such as the individual's knowledge, activity, commitment, and purposes in and places for travel. The section therefore is patently not a regulation narrowly drawn to prevent the supposed evil, yet here, as elsewhere, precision must be the touchstone of legislation so affecting basic freedoms.

*Id.* at 514 (internal quotation marks and citations omitted).

These passport cases did not deal with the limits on governmental authority within the specific context of airline safety, but rather assessed the extent of that authority based on broader national security justifications more directly associated with rights of association and freedom of speech. Nevertheless, when the basic principles discussed in *Kent* and *Aptheker* are applied to the No Fly List, substantial constitutional issues are immediately apparent.

First, the No Fly List, once distributed, clearly infringes upon a citizen's right to travel; and the Court cannot conclude based on the present record that there are no means less restrictive than an unqualified flight ban to adequately assure flight security, such as comprehensive pre-flight screening and searches. Second, the current record is inadequate to explain why judicial involvement before a person is placed on the No Fly List is either unnecessary or impractical, other than perhaps within the context of an emergency based on a specific, imminent threat that requires immediate action. Nor does the record conclusively establish that there cannot be any opportunity, either before or after an American citizen is placed on the No Fly List, to know of or challenge any of the information used to list him, even where such information could be summarized in a way that does not compromise sources or methods.

Third, substantial issues exist concerning the standards used, or required to be used, to determine whether an American citizen can be banned from flying. The process of nomination to the No Fly List is based on a suspected level of future dangerousness that is not necessarily related to any unlawful conduct. In that connection, the TSC's currently applied standard for

inclusion is “satisfaction of a certain substantive derogatory criteria establishing that the individual may be a known or suspected terrorist.” Piehota Decl., ¶ 12. And “[w]hether the individual satisfies the substantive derogatory criteria is generally based on whether there is reasonable suspicion to believe that a person is a known or suspected terrorist.” *Id.* While determining whether a person is a “known terrorist” appears to be straightforward and based on certain formal actions taken within the criminal justice system,<sup>14</sup> whether a person is a “suspected terrorist” appears to be based to a large extent on subjective judgments. As the defendants explain, “[a] suspected terrorist is an individual who is *reasonably suspected* to be, or have been, engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and terrorist activities based on articulable and *reasonable suspicion*.” Piehota Decl., n.5 (emphasis added). In other words, an American citizen can find himself labeled a suspected terrorist because of a “reasonable suspicion” based on a “reasonable suspicion.”

What constitutes conduct sufficiently “related to” or “in aid of” terrorism is not explained, but it is not difficult to imagine completely innocent conduct serving as the starting point for a string of subjective, speculative inferences that result in a person’s inclusion on the No Fly List. For example, is the academic study of terrorism or the investigative reporting of terrorist activities “related to terrorism and terrorist activities”? Is providing financial support to a charitable organization enough, even without knowledge that some of the organization’s activities are “in aid of . . . terrorist activities”? Is it enough to be a member of a lawfully operating social or religious organization whose membership may include other persons

---

<sup>14</sup> “A known terrorist is an individual who has been convicted of, [or is] currently charged with, or under indictment for a crime related to terrorism in a U.S. or foreign court of competent jurisdiction.” Piehota Decl., n.4.



suspected of terrorism? Is studying Arabic abroad, as Mohamed concedes he did, conduct “in preparation for . . . terrorist activities”? A showing of past or ongoing unlawful conduct does not seem to be required, and the level of proof required for inclusion on the No Fly List appears to be far less than that required to obtain such law enforcement tools as a search or arrest warrant or a thirty-day wiretap. *See* U.S. Const. amend. IV; 50 U.S.C. § 1805(a)(2). But the Court has little, if any, ability to articulate what information is viewed by the TSC as sufficiently “derogatory” beyond the labels it has provided the Court.<sup>15</sup>

In sum, the No Fly List assumes that there are some American citizens who are simply too dangerous to be permitted to fly, no matter the level of pre-flight screening or on-flight surveillance and restraint, even though those citizens cannot legally be arrested, detained, or otherwise restricted in their movements or conduct. The No Fly List also assumes that in order to achieve its intended purpose, it must be compiled and distributed without any judicial review or involvement and without any opportunity for the citizen to learn of or contest the accuracy of any information used to justify his inclusion on the list. Specifically at issue in this case is whether, given the substantial liberty interest in freedom of movement possessed by every citizen, the No Fly List, as applied to American citizens, comports with the requirements of substantive and procedural due process.

---

<sup>15</sup> The TSC assures the Court that it does not engage in invidious discrimination “based on race, ethnicity, national origin, religious affiliation, or First Amendment protected activities.” Piehota Decl., ¶ 12. Those assurances, however, do not rule out the possibility, if not probability, that determinations may be bound up with beliefs, personal associations, or activities that are perceived as threatening but are perfectly lawful in themselves, and may indeed be constitutionally protected.

**B. Plaintiff's Claims and Defendants' Objections**

The defendants seek dismissal of Mohamed's claims on both procedural and substantive grounds. First, they argue that Mohamed's claims must be dismissed because he failed to exhaust the available administrative remedies, he lacks standing, and his claims are not ripe for adjudication. Substantively, the defendants contend that: 1) Mohamed has failed to allege a violation of his right to reside in or reenter the United States, and that such a claim is in any event moot; 2) the available administrative remedies satisfy Mohamed's procedural due process rights; and 3) Mohamed's APA claim fails for the same reasons as his other claims and because he makes no allegations supporting a claim of arbitrary and capricious agency action. The Court will address these arguments in turn.

**(1) Exhaustion, Standing, and Ripeness**

The defendants seek dismissal of Mohamed's claims on the ground that he has not presented his claims to the TSA through DHS TRIP and has therefore failed to exhaust administrative remedies. The defendants do not contend that the relevant statutes or regulations require exhaustion, but rather that the Court should require Mohamed to utilize DHS TRIP as a matter of prudence because that process could provide him with some of the relief he seeks and because the Court would be in a better position to review Mohamed's claims after the completion of that process. In a related vein, the defendants contend that Mohamed's constitutional claims are too "hypothetical" to satisfy the requirements of standing and ripeness.

"Where Congress specifically mandates, exhaustion is required." *McCarthy v. Madigan*, 503 U.S. 140, 144 (1992), *superseded by statute on other grounds*. Where exhaustion is not congressionally mandated, on the other hand, "sound judicial discretion" generally governs. *Id.* The Supreme Court has held, however, that a federal court cannot require a plaintiff to exhaust



administrative remedies before seeking judicial review of a final agency action under the APA where neither the relevant statute nor an agency rule imposes such a requirement. *Darby v. Cisneros*, 509 U.S. 137 (1993).

For non-APA claims, “federal courts must balance the interest of the individual in retaining prompt access to a federal judicial forum against countervailing institutional interests favoring exhaustion.” *McCarthy*, 503 U.S. at 146. In that regard, requiring administrative exhaustion allows the agency to “correct its own mistakes with respect to programs it administers before it is haled into federal court” and helps to avoid piecemeal appeals. *Id.* at 145-46. Thus, considerations of efficiency and agency expertise may weigh in favor of requiring exhaustion. *See Guerra v. Scruggs*, 942 F.2d 270, 277 (4th Cir. 1991).

Balancing these conflicting considerations, the Fourth Circuit has recognized that exhaustion should not be required where: (1) exhaustion would be futile; (2) the available administrative remedies would be insufficient; (3) the dispute is a matter of statutory construction; (4) compelling the use of administrative procedures would cause irreparable injury; or (5) requiring exhaustion would leave an administrative decision unreviewed. *See Darby v. Kemp*, 957 F.2d 145, 147 (4th Cir. 1992), *overruled on other grounds*, *Darby v. Cisneros*, 509 U.S. 137 (1993); *McDonald v. Centra, Inc.*, 946 F.2d 1059, 1063 (4th Cir. 1991). Because administrative remedies are almost always inadequate to address procedural due process challenges to those remedies, such challenges are particularly immune from administrative exhaustion requirements. *See Bangura v. Hansen*, 434 F.3d 487, 494 (6th Cir. 2006) (“Exhaustion of administrative remedies may not be required in cases of non-frivolous constitutional challenges to an agency’s procedures.”); *see also Gibson v. Berryhill*, 411 U.S. 564, 575 (1973) (holding that appellee was not required to exhaust state administrative remedies

where “the question of the adequacy of the administrative remedy . . . was for all practical purposes identical with the merits of appellees’ lawsuit”); *Kreschollek v. S. Stevedoring Co.*, 78 F.3d 868, 875 (3d Cir. 1996) (holding that exhaustion of administrative remedies under the Longshore and Harbor Workers’ Compensation Act was not required where the administrative process was inadequate to address the Longshoreman’s claim that the Act unconstitutionally deprived him of a hearing prior to the deprivation of benefits).

The Court concludes that it would be inappropriate to require exhaustion in this case. First, as the defendants acknowledge, Congress has not mandated exhaustion of the DHS TRIP process with respect to Mohamed’s claims, and there are no regulations regarding DHS TRIP that mandate exhaustion. *See* 49 U.S.C. §§ 44903(j)(2) & 44926(a) (directing DHS to create a redress program without requiring that travelers take advantage of it). It would therefore appear that the Court could not, under the holding in *Darby v. Cisneros*, require Mohamed to exhaust the DHS TRIP process before proceeding with his APA appeal in Count II. To require exhaustion with respect to Mohamed’s other claims, then, would essentially bifurcate substantially related, if not common, claims and create, rather than avoid, piecemeal litigation.

Second, it is difficult to see how exhaustion of DHS TRIP would significantly assist the Court in adjudicating or resolving Mohamed’s claims. Mohamed would not have access to any information the government used to place him on the No Fly List, and once the government completed the review, he would receive only a letter indicating that the review process was complete. He would not receive any substantive information as to whether he was, or ever had been, on the No Fly List, or the grounds for his potential inclusion on the list. For these reasons, Mohamed would not have any opportunity to respond to the information used by the government to place him on the No Fly List; and it is not even clear whether he would have any meaningful

opportunity to submit and have considered information that might negate any “derogatory information” possessed by the government, even without access to the government’s reasons for his inclusion on the No Fly List.

Moreover, DHS TRIP would not provide Mohamed with any opportunity to present and have considered his constitutional claims. That process addresses only whether a traveler who has submitted an inquiry is in fact the individual listed in the TSDB, and if so, whether there is sufficient information to support the listing. As a result, at the end of the DHS TRIP process, even were the TSC to voluntarily remove Mohamed from the No Fly List, the alleged underlying constitutional infirmities that allowed his name to be included on the list and distributed to airlines would remain in place, unreviewed and with no assurances that Mohamed would not suffer the same alleged injury in the future.<sup>16</sup> In other words, the administrative process that the defendants want exhausted would not address Mohamed’s constitutional claims.

Finally, the Court has no expectation that the DHS TRIP process would create a record more helpful than the one that already exists.<sup>17</sup> According to the government, if Mohamed is on

---

<sup>16</sup> As mentioned above, the letters sent by the TSA at the conclusion of the review process indicate that review is available pursuant to 49 U.S.C. § 46110, which provides for review of TSA orders in the Courts of Appeals. The defendants have represented to the Court that, should Mohamed choose to appeal after completing the DHS TRIP process, they would provide to the Court of Appeals an “administrative record” that the Court could review *in camera*. In reversing this Court’s August 2011 Order, however, the Court of Appeals reasoned that it lacked exclusive jurisdiction under 49 U.S.C. § 46110 because “resolving substantive and procedural due process challenges to an individual’s inclusion on the No-fly list necessarily requires scrutiny of both the TSC’s and the TSA’s actions,” and the Court would be unable to “directly review the TSC’s actions, direct the agency to develop necessary facts or evidence, or compel its compliance with any remedy [the court] might fashion.” Slip op. at 5-6. Those same considerations would apply were Mohamed to appeal after completion of the DHS TRIP process, indicating that such an appeal would not provide adequate review of Mohamed’s constitutional claims.

<sup>17</sup> In *Shearson v. Holder*, 725 F.3d 588, 593-95 (6th Cir. 2013), relied upon heavily by the defendants, the Sixth Circuit held that the plaintiff, who alleged she was detained at the United

the No Fly List, there already exists for the Court's review an administrative file containing the "derogatory information" the TSC relied upon in placing him on the list. *See* Piehota Decl., ¶ 9. There is also no reason to think that the DHS TRIP process would develop any of the additional factual record relevant for the purposes of Mohamed's constitutional claims, given the limited scope of the issues addressed in DHS TRIP.<sup>18</sup>

As for standing, Mohamed's alleged constitutional injuries constitute an "injury in fact" that is actual, concrete and particularized, and traceable to the defendants, who are alleged to be responsible for placing him on the No Fly List and distributing it to the TSA.<sup>19</sup> Further, the relief Mohamed seeks, including removal from the No Fly List, would redress his alleged injury.<sup>20</sup> As

---

States boarder due to her inclusion in the TSDB, could not pursue her procedural due process claim before seeking relief through DHS TRIP. The court in *Shearson* reasoned that it was appropriate to require exhaustion because the plaintiff might be removed from the TSDB and because the review process would "create a record that may be reviewed by a judge *in camera*." *Id.* at 595. Based on the particular facts and circumstances of this case, the Court finds that neither possibility justifies requiring exhaustion in this case.

<sup>18</sup> Also militating against exhaustion in this case is Mohamed's interest in a prompt adjudication of his claims, first filed more than two years ago, and the lack of any time requirement for the government to complete the DHS TRIP process, coupled with the defendants' inability to provide to the Court any actual estimate of how long that process would take. *See Coit Indep. Joint Venture v. Fed. Sav. & Loan Ins. Corp.*, 489 U.S. 561, 586-87 (1989) (holding that available administrative remedy was inadequate, and therefore declining to require exhaustion, where administrative agency was not required to render a decision within a reasonable time limit).

<sup>19</sup> To establish standing, a plaintiff must show that: (1) he has suffered an injury in fact that is "concrete and particularized" and "actual or imminent"; (2) the injury is "fairly ... trace[able] to the challenged action of the defendant"; and (3) it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (internal quotation marks omitted).

<sup>20</sup> The defendants contend that Mohamed lacks standing because he "cannot be allowed to invoke the jurisdiction of this Court by refusing to avail himself of an existing administrative process that may address his alleged harm." Defendants' Memorandum in Support of Motion to Dismiss Plaintiff's Third Amended Complaint (hereinafter "Memorandum in Support") at 13.

to ripeness, there is nothing “hypothetical” about Mohamed’s claims, which attack the constitutionality of the No Fly List.<sup>21</sup> The DHS TRIP process is already established, and Mohamed’s participation in the process would not provide the Court with more information about how the process works than the Court already possesses or could be presented at trial. In the end, the defendants’ standing and ripeness challenges are bound up with their exhaustion position and fail for essentially the same reasons. Thus, the Court concludes that Mohamed has standing and his claims are ripe.

**(2) Defendants’ Contention that Plaintiff Fails to State a Claim**

**a. Count I: Citizen’s Right to Reenter the United States**

In Count I, styled “Violation of U.S. Citizen’s Right to Reside in United States and to Reenter the United States from Abroad,” Mohamed alleges that, “[b]y placing [him] on the No Fly List while he was abroad, Defendants Unknown TSC Agents prevented [him] from boarding an aircraft to return to the United States, even though no other means existed by which he may return to the United States, thus violating [his] constitutional rights.” Third Amend. Compl. ¶

---

But the cases the defendants cite in support of this position are inapposite, and simply restrict plaintiffs who have failed to take advantage of an available process that “appears to provide due process” from “us[ing] the federal courts as a means to get back what [they] want.” *Wilson v. MVM, Inc.*, 475 F.3d 166, 176 (3d Cir. 2007) (internal quotation marks omitted). Here, Mohamed does not seek to bypass ostensibly adequate procedural remedies; rather, he challenges the constitutionality of those remedies, which, by the defendants’ own description, do not allow him to raise and have considered his constitutional challenges.

<sup>21</sup> The “basic rationale” of the ripeness doctrine is “to prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements.” *Ostergren v. Cuccinelli*, 615 F.3d 263, 288 (4th Cir. 2010) (quoting *Abbott Labs. v. Gardner*, 387 U.S. 136, 148 (1967)). The court assesses ripeness by “balanc[ing] the fitness of the issues for judicial decision with the hardship to the parties of withholding court consideration.” *Id.* (quoting *Miller v. Brown*, 462 F.3d 312, 319 (4th Cir. 2006)). The defendants argue that, without requiring Mohamed to submit to the DHS TRIP process, “the Court would be ruling on the hypothetical deficiencies of a process that the Plaintiff has not tested and would be without the benefit of the agency’s expert assessment.” Memorandum in Support at 13.

56. Further, Mohamed alleges that, by maintaining him on the No Fly List, the defendants have “substantially burdened his fundamental right to return to the United States in the immediate future.” *Id.* ¶ 57. Count I is, in essence, a substantive due process claim.

Substantive due process “provides heightened protection against government interference with certain fundamental rights and liberty interests.” *Washington v. Glucksberg*, 521 U.S. 702, 719 (1997). Those protected rights and interests include those that “are, objectively, deeply rooted in this Nation’s history and tradition, and implicit in the concept of ordered liberty, such that neither liberty nor justice would exist if they were sacrificed.” *Id.* at 720–21 (internal quotation marks and citations omitted). In contrast to the procedural component of the Due Process Clause, substantive due process “protects individual liberty against certain government actions regardless of the fairness of the procedures used to implement them.” *Collins v. City of Harker Heights*, 503 U.S. 115, 125 (1992) (internal quotation marks omitted).

The defendants do not contest that a United States citizen has a right to reenter the United States. They contend, however, that Count I must fail because the right of reentry attaches only once a citizen presents himself at a U.S. port of entry and does not extend to restrictions that may prevent or impede his ability to reach a U.S. port of entry. Based on this position, the defendants contend that, as a matter of law, based on his allegations, Mohamed has never been denied reentry to the United States, and that, even if he is on the No Fly List, Mohamed will not in the future be denied reentry once he presents himself at the border.

The Court concludes that a U.S. citizen’s right to reenter the United States entails more than simply the right to step over the border after having arrived there. *See, e.g., Newton v. INS*, 736 F.2d 336, 343 (6th Cir. 1984) (noting that citizens “have the right to *return* to this country at any time of their liking” (emphasis added)). At some point, governmental actions taken to



prevent or impede a citizen from reaching the boarder infringe upon the citizen's right to reenter the United States. The issue is whether the defendants' conduct has in the past or will in the future cross over into an unconstitutional burden on that right of reentry.

Mohamed invokes his right of reentry with respect to both his initial unsuccessful attempt to return to the United States from Kuwait in January 2011 and also with respect to his plans to travel abroad for religious purposes and to visit his family. As to his claim of past constitutional injury, the Court concludes that Mohamed has failed to allege facts that make plausible his claim that his constitutional right of reentry was violated when he was prevented from boarding a plane from Kuwait to the United States on January 16, 2011 because of his placement on the No Fly List. Mohamed's own allegations establish that, although he was denied boarding on that flight, he was able to board a flight on January 20, 2011 and reenter the United States without incident on January 21, 2011. Even accepting as true Mohamed's allegations—including that the government improperly placed him on the No Fly List and prevented him from boarding the January 16th flight—the four to five-day delay that Mohamed experienced in his ability to reenter the United States did not unduly burden his right of reentry and therefore, as a matter of law, did not constitute a constitutional deprivation.

Broader, however, are Mohamed's allegations of present and future harms arising from his inability to fly. In that regard, Mohamed alleges that, even though the defendants permitted his return in January 2011, his continued inclusion on the No Fly List presumptively prevents him from departing the United States to travel abroad for a religious pilgrimage and to visit family members, and, were he able to leave the United States, from returning to the country through any practical means. Thus, Mohamed complains of a violation of his right to exit and return based on the burden placed on his right to international travel, which, as discussed above,

is “an important aspect of the citizen's ‘liberty’ guaranteed in the Due Process Clause of the Fifth Amendment.” *Aptheker*, 378 U.S. at 505 (quoting *Kent*, 357 U.S. at 127). It is true that the right to international travel is not, like the right to interstate travel, “virtually unqualified,” but rather is subject to “reasonable governmental regulation.” *Haig v. Agee*, 453 U.S. 280, 306-307 (1981) (citation omitted). Nonetheless, “a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.” *Aptheker*, 378 U.S. at 508 (quoting *NAACP v. Alabama*, 377 U.S. 288, 307 (1964)). Whether Mohamed’s alleged disabilities as a result of his alleged inclusion on the No Fly List unconstitutionally burden the exercise of his right of exit and reentry cannot be decided at this stage as a matter of law. However, Mohamed’s factual allegations, taken as true, suffice to make plausible his substantive due process claim.

**b. Count III: Procedural Due Process**

In Count III, Mohamed alleges that the defendants have failed to provide him with “a meaningful opportunity to challenge his inclusion on the No Fly List either prior or subsequent to his placement, depriving him of his liberty interest in (1) being able to return to the United States, (2) traveling by air like other American citizens, and (3) being free from false governmental stigmatization as a terrorist.” Third Amend. Compl. ¶ 62. The defendants contend that “the redress process available through DHS TRIP is constitutionally sufficient to address Plaintiff’s claims, given the limited private interest at issue, the profound government interest in protecting the security of civil aviation, and the negligible value of additional measures given the robust internal review of highly sensitive information by experts tasked with protecting national



security.” Defendants’ Memorandum in Support of Motion to Dismiss Plaintiff’s Third Amended Complaint at 16.

“The fundamental requirement of due process is the opportunity to be heard at a meaningful time and in a meaningful manner.” *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976) (internal quotation marks omitted). However, “[t]he procedural protections required by the Due Process Clause must be determined with reference to the rights and interests at stake in the particular case.” *Washington v. Harper*, 494 U.S. 210, 229 (1990). In evaluating the sufficiency of the process the government has provided in a particular case, the Court must consider: (1) “the private interest that will be affected by the official action”; (2) “the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards”; and (3) “the Government’s interest.” *Mathews*, 424 U.S. at 335. These factors, when considered within the context of Mohamed’s allegations, necessarily require an evidentiary record beyond that presented to the Court in connection with the defendants’ motion to dismiss.

As discussed above, Mohamed alleges a range of protectable interests, including his right to travel, that have been affected adversely by his alleged inclusion on the No Fly List.<sup>22</sup>

---

<sup>22</sup> Central to the defendants’ defense of the No Fly List is their contention that there is no fundamental right to the most convenient form of travel. See Memorandum in Support at 18-19 (citing, e.g., *Gilmore v. Gonzales*, 435 F.3d 1125, 1136-37 (9th Cir. 2006) (holding that airline policy requiring identification to fly did not unreasonably burden right to interstate travel); *Miller v. Reed*, 176 F.3d 1202, 1205-1206 (9th Cir. 1999) (indicating that there is no fundamental right to drive); *Cramer v. Skinner*, 931 F.2d 1020, 1031 (5th Cir. 1991) (“Minor restrictions on travel simply do not amount to the denial of a fundamental right that can be upheld only if the Government has a compelling justification.”). As discussed above, the constitutional issues presented by the No Fly List, as it applies to American citizens, go far beyond any claimed right to travel by the most convenient means. In any event, in none of the cases the defendants cite was the plaintiff deprived entirely of the right to travel by air. See *Gilmore*, 435 F.3d at 1137 (challenge to identification policy requiring airline passengers to

Further, the government's interest in combating terrorism is no doubt substantial. The Court must then determine whether the No Fly List and the redress procedures provided through DHS TRIP constitute appropriate means to prevent terrorism directed against air travel while protecting the liberty interests at stake. By the defendants' own account, individuals are placed in the TSDB according to a reasonable suspicion standard and without any judicial involvement. Nominations to the No Fly List must satisfy "additional derogatory requirements," Pichota Decl., ¶ 10, but it is unclear what these are. Regardless, it does not appear that unlawful conduct, unlawful speech, or unlawful association is required.

As the defendants have also acknowledged, an individual placed on the No Fly List does not receive any notice of his placement on the list, pre-deprivation or otherwise, or the reasons for his inclusion. Further, an individual's inclusion on the No Fly List and the dissemination of that list are accomplished without any judicial involvement or review, and according to a standard of proof that is far less than that typically required when the deprivation of significant constitutional liberties are implicated. While the government no doubt has a significant and even compelling interest, an American citizen placed on the No Fly List has countervailing liberty interests and is entitled to a meaningful opportunity to challenge that placement. And, while judicial review of some sort is available pursuant to 49 U.S.C. § 46110, as discussed above, it is not at all clear that such review will effectively address the constitutional issues presented by a citizen's inclusion on the No Fly List. Finally, the defendants have not made a sufficient

---

present identification or be subjected to more extensive searches); *Cramer*, 931 F.2d at 1029-33 (challenge to law that restricted interstate air service from a particular airport); *City of Houston v. FAA*, 679 F.2d 1184, 1198 (5th Cir. 1982) (challenge to regulations prohibiting air carriers from operating nonstop flights between Washington National Airport and any airport more than 1,000 miles away).

showing at this point that they could not accomplish their objectives using less restrictive means, such as enhanced screening.

For these reasons, the Court cannot conclude, as a matter of law, that DHS TRIP provides sufficient process to defeat Mohamed's procedural due process claim, and instead must conclude that Mohamed has alleged facts sufficient to make that claim plausible. In resolving the claim, the Court must engage in a fact-intensive consideration of the personal liberties involved, the government's compelling interest in combating terrorism, the procedures used in connection with the No Fly List, and the use made of the No Fly List.


c. Count II: Administrative Procedure Act

In Count II of his Third Amended Complaint, in addition to reiterating his constitutional claims, Mohamed alleges that "Defendants' actions described herein were and are arbitrary, capricious, an abuse of discretion, otherwise not in accordance with law, and contrary to constitutional right and should be set aside as unlawful pursuant to 5 U.S.C. § 706." Third Amend. Compl. ¶ 59. The issues presented in Mohamed's APA claim essentially conflate with his constitutional claims. Thus, for the same reasons discussed above the Court concludes that Mohamed's factual allegations make plausible his claim that the defendants' actions were arbitrary and capricious, an abuse of discretion, or otherwise not in accordance with law.

**III. CONCLUSION**

For the reasons stated above, the defendants' Motion to Dismiss will be GRANTED in part and DENIED in part. The Motion will be granted as to Plaintiff's claim in Count I of his Third Amended Complaint that he was denied his constitutional right of reentry in January 2011, and will otherwise be DENIED.

An appropriate Order will issue.

---

Anthony J. Tien  
United States District Judge

Alexandria, Virginia  
January 22, 2014

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

PLAINTIFF'S  
EXHIBIT

2

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## 2013 WATCHLISTING GUIDANCE TABLE OF CONTENTS

<b>CHAPTER 1: WATCHLISTING PROCESS AND PROCEDURES .....</b>	<b>5</b>
I. INTRODUCTION.....	5
II. WATCHLISTING AUTHORITIES .....	6
III. CONSTITUTIONALLY PROTECTED ACTIVITIES .....	10
IV. WATCHLISTING POLICIES .....	11
V. WATCHLISTING STANDARD: IDENTIFYING AND SUBSTANTIVE DEROGATORY CRITERIA .....	12
VI. WATCHLISTING PROCESS OVERVIEW.....	13
VII. ROLES AND RESPONSIBILITIES FOR THE WATCHLISTING AND SCREENING COMMUNITY .....	16
VIII. QUALITY CONTROL MEASURES .....	17
IX. NOMINATION PROCEDURES .....	20
X. PROCEDURES TO REMOVE AN INDIVIDUAL FROM THE WATCHLIST ...	27
XI. REDRESS PROCEDURES.....	28
XII. PERIODIC REVIEW OF THE WATCHLISTING GUIDANCE .....	29
<b>CHAPTER 2: MINIMUM IDENTIFYING CRITERIA.....</b>	<b>30</b>
I. BIOMETRIC NOMINATIONS.....	30
II. MINIMUM BIOGRAPHIC NOMINATION REQUIREMENT .....	30
III. MINIMUM BIOGRAPHIC INFORMATION REQUIRED FOR EXCEPTIONS TO THE	

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

MINIMUM SUBSTANTIVE DEROGATORY STANDARDS FOR TERRORIST WATCHLISTING.....	32
---	----

**CHAPTER 3: MINIMUM SUBSTANTIVE DEROGATORY CRITERIA .....33**

I. INTRODUCTION AND PURPOSE .....	33
II. REASONABLE SUSPICION.....	33
III. KNOWN TERRORISTS.....	35
IV. SUSPECTED TERRORISTS .....	37
V. EXCEPTIONS TO SUPPORT IMMIGRATION AND VISA SCREENING ACTIVITIES BY DHS AND DOS.....	42
VI. SPECIAL CONSIDERATIONS .....	45
VII. EXAMPLES OF TERRORISM AND/OR TERRORIST ACTIVITIES.....	47

**CHAPTER 4: NO FLY, SELECTEE AND EXPANDED SELECTEE LISTS  
IMPLEMENTATION GUIDANCE.....50**

I. BACKGROUND.....	50
II. PRE-CONDITIONS FOR PLACEMENT ON THE NO FLY OR SELECTEE LIST.	50
III. NO FLY LIST CRITERIA.....	51
IV. FURTHER CLARIFICATION OF NO FLY CRITERIA .....	51
V. SELECTEE LIST CRITERIA .....	54
VI. EXPANDED SELECTEE LIST CRITERIA .....	54
VII. ACTIONS BASED UPON POSITIVE MATCHES TO THE NO FLY, SELECTEE, OR EXPANDED SELECTEE LISTS .....	54
VIII. IMPLEMENTATION GUIDELINES .....	55

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

IX.	SPECIAL SITUATIONS .....	56
X.	NOMINATIONS THAT ARE INELIGIBLE/NOT SUITABLE FOR EITHER THE NO FLY OR THE SELECTEE LIST .....	57

## CHAPTER 5: ENCOUNTER MANAGEMENT AND ANALYSIS ..... 58

I.	INTRODUCTION AND PURPOSE .....	58
II.	PROCESSING TERRORISM INFORMATION FROM ENCOUNTERS WITH POSITIVELY IDENTIFIED KNOWN OR SUSPECTED TERRORISTS .....	59
III.	CATEGORIES OF TERRORISM INFORMATION FROM ENCOUNTERS WITH POSITIVELY IDENTIFIED KNOWN OR SUSPECTED TERRORISTS OF POTENTIAL INTEREST .....	65
IV.	ENCOUNTER MANAGEMENT ACTIONS .....	69
V.	ROLES AND RESPONSIBILITIES FOR UPDATING EXISTING KNOWN OR SUSPECTED TERRORIST RECORDS AND NOMINATING NEW KNOWN OR SUSPECTED TERRORISTS BASED ON INFORMATION FROM POSITIVE ENCOUNTERS .....	71
VI.	RESPONSIBILITY TO COORDINATE ANY ACTIONS CONTEMPLATED BASED ON INFORMATION FROM ENCOUNTERS WITH A KNOWN OR SUSPECTED TERRORIST .....	73
VII.	EXAMPLES OF TERRORISM INFORMATION TYPICALLY AVAILABLE FROM ENCOUNTERS .....	74
VIII.	OBTAINING ENCOUNTER INFORMATION THROUGH TSC'S DAILY ENCOUNTER REPORTS .....	77

### APPENDIX 1: DEFINITIONS

### APPENDIX 2: HSPD-6

### APPENDIX 3: TSC MOU

### APPENDIX 4: ADDENDUM B TO TSC MOU

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**APPENDIX 5: INFORMATION SHARING MOU**

**APPENDIX 6: EXECUTIVE ORDER 13388**

**APPENDIX 7: DOJ PROTOCOL ON TERRORIST NOMINATIONS**

**APPENDIX 8: REDRESS MOU**

**APPENDIX 9: PRESIDENTIAL MEMORANDUM REGARDING 12/25/2009 TERRORIST  
ATTACK**

**APPENDIX 10: ACRONYMS AND ABBREVIATIONS**

**APPENDIX 11: SUMMARY OF CHANGES AND UPDATES FROM THE 2010  
WATCHLISTING GUIDANCE**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## CHAPTER 1: WATCHLISTING PROCESS AND PROCEDURES

## I. INTRODUCTION

- 1.1 A key foundation for TERRORIST<sup>1</sup>-related screening is the U.S. Government's TERRORIST watchlisting process managed by the Terrorist Screening Center (TSC). The TSC was established by the Attorney General, acting through the Director of the Federal Bureau of Investigation (FBI), and in coordination with the Secretary of State, the Secretary of Homeland Security, and the then Director of Central Intelligence for the Intelligence Community (IC). The TSC is supported by the National Counterterrorism Center (NCTC), the Department of State (DOS), the Department of Homeland Security (DHS), the IC, the FBI, Law Enforcement Agencies, Regulatory Agencies and Diplomatic Bureaus. The TSC has created and maintains the Terrorist Screening Database (TSDB) or Terrorist Watchlist to serve as the U.S. Government's consolidated watchlist for TERRORISM SCREENING INFORMATION.
- 1.2 The current TERRORIST watchlisting process supports the U.S. Government's efforts to combat TERRORISM by: (1) consolidating the U.S. Government's Terrorist Watchlist in the TSDB; (2) helping SCREENERS and intelligence agencies accurately identify individuals on the Terrorist Watchlist; (3) providing SCREENERS with information to help them respond appropriately during ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS; and, (4) subsequently collecting information about the KNOWN or SUSPECTED TERRORIST for use in assessing threats and conducting investigations.<sup>2</sup> The collected information may be incorporated into the Terrorist Identities Datamart Environment (TIDE) and TSDB to enhance the records of KNOWN or SUSPECTED TERRORISTS and may be made available to the wider watchlisting and screening communities. Today, the TSDB also includes information about certain foreign nationals who are associated with TERRORISM, TERRORIST ACTIVITY, or KNOWN or SUSPECTED TERRORIST(S) but for whom there is insufficient DEROGATORY INFORMATION to be independently watchlisted. This may include certain immediate family members of KNOWN or SUSPECTED TERRORISTS, or known associates of KNOWN or SUSPECTED TERRORISTS. These additional categories of records (also known as exceptions to the REASONABLE SUSPICION standard) are maintained to support immigration and screening activities primarily conducted by DOS and DHS.<sup>3</sup>

<sup>1</sup> See Appendix 1, Definitions for words or phrases appearing in all capitalized letters throughout this Watchlisting Guidance.

<sup>2</sup> A SCREENER is a Department or Agency that is authorized to conduct TERRORISM screening to determine if an individual is a possible match to a KNOWN or SUSPECTED TERRORIST in the TSDB. The term "SCREENER" is used throughout this document as a general reference to a government official who compares an individual's information with information in the TSDB to determine if an individual is in the TSDB. Certain SCREENERS have components which perform both screening and law enforcement duties and law enforcement officials who engage in such activities may normally describe their targeting or other actions in this context as other than "screening." For ease of reference, government officials who compare an individual's information with information in the TSDB will be referred to in the Guidance as "SCREENERS." The internal guidance set forth herein is not intended to create or confer any rights, privileges, or benefits in any matter, case, or proceeding. See *United States v. Caceres*, 440 U.S. 741.

<sup>3</sup> See Chapter 3, Section V, *infra*, for more details. Aside from these limited exceptions, references to the TSDB in this Watchlisting Guidance denote the TSDB as containing information about KNOWN or SUSPECTED TERRORISTS.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 1.3 This Watchlisting Guidance has been developed to help standardize the watchlisting community's nomination and screening processes. It is important to remember, however, that watchlisting is not an exact science. There are inherent limitations in any primarily name-based system and analytic judgments may differ regarding whether subjective criteria have been met. Given these realities, the U.S. Government's watchlisting process attempts to safeguard the American people from a TERRORIST attack while safeguarding privacy, civil rights and civil liberties.
- 1.4 Thus, when reasonable minds could disagree on a record, a NOMINATOR will make a determination in favor of sending the nomination to NCTC for consideration and additional review. The TSC has the final decision authority regarding watchlisting determinations and will add an individual's name to the TSDB, consistent with TSC Actions and Processes as further described in Paragraph 1.56.

**II. WATCHLISTING AUTHORITIES**

- 1.5 On September 16, 2003, the President issued Homeland Security Presidential Directive 6 (HSPD-6), which directed the Attorney General to "establish an organization to consolidate the U.S. Government's approach to TERRORISM SCREENING and provide for the appropriate and lawful use of TERRORIST INFORMATION in screening processes."<sup>4</sup> TERRORIST INFORMATION was specifically defined to mean "information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM." HSPD-6 also directed the heads of Executive Departments and Agencies to provide to NCTC on an on-going basis, "all appropriate TERRORIST INFORMATION in their possession, custody, or control," to the extent permitted by law.
- 1.6 The intent of HSPD-6 was to consolidate all TERRORISM INFORMATION at the Terrorist Threat Integration Center (TTIC) – whose functions were assumed by NCTC<sup>5</sup> – in a classified database that would then extract Unclassified, For Official Use Only (U//FOUO) TERRORIST IDENTIFIERS for passage to the new organization created by the Attorney General. Thus, concurrent with the issuance of HSPD-6, the TSC was established via the *Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (TSC MOU)*, which was signed by the Attorney General, the Secretaries of State and Homeland Security, and the Director of Central Intelligence (on behalf of the IC).<sup>6</sup>

---

<sup>4</sup> See Appendix 2, HSPD-6.

<sup>5</sup> See FN 8, *infra*.

<sup>6</sup> See Appendix 3, *TSC MOU*; see also Appendix 4, Addendum B to the *TSC MOU*. In 2004, the Secretaries of State, Treasury, and Defense also became signatories to the *Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing*, dated March 4, 2003 (*Information Sharing MOU*). By doing so, they agreed that all provisions of the *TSC MOU* and the *Information Sharing MOU* apply to all entities that are or become a part of their respective Departments.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 1.7 Under HSPD-6, consistent with the U.S. Constitution and applicable laws, including those protecting the rights of all Americans, the TSC was to develop and maintain an unclassified database containing the most thorough, accurate, and current identity information possible about KNOWN or SUSPECTED TERRORISTS. The TSC created the TSDB to meet these goals.<sup>7</sup> The TSDB is also known as the Terrorist Watchlist. The TSDB receives TERRORIST IDENTIFIERS from two sources: NCTC's TIDE provides information concerning KNOWN or SUSPECTED international TERRORISTS and the TSC's Terrorist Review and Examinations Unit (TREX) provides the identities of KNOWN or SUSPECTED domestic TERRORISTS who have no link to international TERRORISM. NCTC's TIDE contains identifying and substantive DEROGATORY INFORMATION on KNOWN or SUSPECTED international TERRORISTS and the FBI's Sentinel system contains supporting information regarding purely domestic TERRORISTS.
- 1.8 Pursuant to Paragraph (2) of HSPD-6, the NCTC is mandated to "provide [TSC] with access to all appropriate information or intelligence in the [NCTC's] custody, possession, or control that [TSC] requires to perform its functions." NCTC fulfills this function by providing TSC's TSDB with U//FOUO information about KNOWN or SUSPECTED TERRORISTS from NCTC's TIDE and by providing access to TIDE Online, a read-only copy of the TIDE database, to those in the watchlisting community who require access.
- 1.9 NCTC's establishment by the President was codified by section 1021 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).<sup>8</sup> Pursuant to IRTPA, NCTC shall "serve as the central and shared knowledge bank on KNOWN and SUSPECTED TERRORISTS and international terror groups." In addition, NCTC "may, consistent with applicable law, the direction of the President, and guidelines referred to in [the statute], receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence."<sup>9</sup>
- 1.9.1 All Departments and Agencies are required to provide NCTC with all TERRORISM INFORMATION. Due to the amount of information involved, only a subset of this information is provided in the NCTC prescribed format designed to facilitate direct ingestion into the TIDE. NOMINATING DEPARTMENTS and AGENCIES, however, should remain focused on reviewing and watchlisting TERRORISM INFORMATION from datasets most likely to contain information about KNOWN or SUSPECTED TERRORISTS.

---

Addendum B to the TSC MOU, which superseded Addendum A, incorporates by reference all provisions of the *Information Sharing MOU*. See Appendix 5.

<sup>7</sup> The TSDB consolidates the U.S. Government's TERRORISM screening and lookout databases into a single integrated TERRORIST identities database.

<sup>8</sup> NCTC initially was created by Executive Order 13354 (August 27, 2004) to serve as the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to TERRORISM and counterterrorism, excepting purely domestic counterterrorism information. Executive Order 13354 was revoked by Executive Order 13470 (July 30, 2008) after NCTC was codified in IRTPA section 1021.

<sup>9</sup> In addition to the provision of domestic KNOWN or SUSPECTED TERRORISTS directly to the TSC, the TSC's TREX unit also provides the identities of international KNOWN or SUSPECTED TERRORISTS to NCTC for inclusion in TIDE.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 1.10 On August 27, 2004, the President issued Homeland Security Presidential Directive 11 (HSPD-11), which “builds upon HSPD-6,” to enhance TERRORIST-related screening to more effectively detect and interdict SUSPECTED TERRORISTS and TERRORIST ACTIVITIES. HSPD-11 defines “SUSPECTED TERRORISTS” as “individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM . . . and TERRORIST ACTIVITIES.”
- 1.11 To enhance information sharing, another key component of the consolidated terrorist watchlisting system, the President issued Executive Order 13388, which provides that the head of each Agency that possesses or acquires TERRORISM INFORMATION shall promptly give access to that information to the head of each other Agency that has counterterrorism functions.<sup>10</sup>
- 1.12 On June 5, 2008, the President issued Homeland Security Presidential Directive 24 (HSPD-24) to further build upon the TERRORIST screening policies announced in HSPD-6 and HSPD-11 to protect the nation from TERRORISTS by enhancing the use of biometrics. In HSPD-24, the President directed that “. . . agencies, shall, to the fullest extent permitted by law, make available to other agencies all biometric and associated biographic and contextual information associated with persons *for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security*” (emphasis added). HSPD-24 underscores the value of biometrics in achieving effective TERRORISM screening and emphasizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient.
- 1.13 The relevant TERRORISM screening Presidential Directives use words and phrases to describe a KNOWN or SUSPECTED TERRORIST subject to TERRORIST screening without defining them: “TERRORIST INFORMATION” (HSPD-6), “TERRORISM” (HSPD-6), “appropriately suspected” (HSPD-6), “reasonably suspected” (HSPD-11), and “articulable and reasonable basis for suspicion” (HSPD-24). Thus, previous watchlisting guidance supplied definitions of key terms and the standard that would apply to terrorist watchlisting decisions.
- 1.14 Neither HSPD-6 nor HSPD-11 defines “TERRORISM and/or TERRORIST ACTIVITIES.” While federal law contains numerous definitions of “terrorism”<sup>11</sup>, for watchlisting purposes under this Guidance, “TERRORISM and/or TERRORIST ACTIVITIES” combine elements from various federal definitions and are considered to:

- 1.14.1 involve violent acts or acts dangerous to human life, property, or infrastructure

<sup>10</sup> See Appendix 6, Executive Order 13388.

<sup>11</sup> See 50 U.S.C. 1801(c) (Foreign Intelligence Surveillance Act (FISA) definition of “international terrorism”); Immigration and Nationality Act (INA) § 212(a)(3)(B)(iii) [8 U.S.C. 1182(a)(3)(B)(iii)] (defining “terrorist activity”); INA § 212(a)(3)(B)(iv) [8 U.S.C. 1182(a)(3)(B)(iv)] (defining to “engage in terrorist activity”); 18 U.S.C. 2331(1) (defining “international terrorism”); 18 U.S.C. 2332(b) (defining “federal crime of terrorism”); Executive Order 13224, 66 Fed. Reg. 49079 (September 23, 2001) (defining “terrorism”).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

which may be a violation of U.S. law, or may have been, if those acts were committed in the United States; and,

1.14.2 appear to be intended—

1.14.2.1 to intimidate or coerce a civilian population;

1.14.2.2 to influence the policy of a government by intimidation or coercion; or,

1.14.2.3 to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

1.15 This includes activities that facilitate or support TERRORISM and/or TERRORIST ACTIVITIES such as providing a safe house, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training for the commission of an act of TERRORISM and/or TERRORIST ACTIVITY.

1.16 HSPD-24 speaks in terms of “articulable and reasonable basis for suspicion” to describe a KNOWN or SUSPECTED TERRORIST who should be watchlisted and represents the President’s most recent explanation concerning U.S. policy regarding the individuals who pose a threat to national security and should be screened to better protect the American people. Accordingly, that standard has been adopted and is clarified in this Watchlisting Guidance in Chapter 3, Section II.

1.17 On December 16, 2005, in accordance with section 1016 of IRTPA, the President issued a Memorandum for the Heads of Executive Departments and Agencies prescribing the guidelines and requirements in support of the creation and implementation of the Information Sharing Environment (ISE). In Guideline 5 of that Memorandum, the President directed, as he had earlier in Executive Order 13353<sup>12</sup>, that the information privacy rights and other legal rights of Americans must be protected and that guidelines be developed and approved to ensure that “such rights are protected in the development and use of the ISE.” In December 2006, the President approved for issuance the *ISE Privacy Guidelines* by the Program Manager.<sup>13</sup>

1.18 A second addendum to the *TSC MOU*, Addendum B<sup>14</sup>, which supplements and incorporates by reference all provisions of the *TSC MOU*, superseded Addendum A and became effective on January 18, 2007. The Directors of National Intelligence, NCTC, and the TSC joined as signatories in Addendum B. Paragraph 7 of Addendum B introduces the term TERRORIST IDENTIFIERS to more clearly describe the type of TERRORIST identity elements that are deemed

<sup>12</sup> See Executive Order 13353, Establishing the President’s Board on Safeguarding Americans’ Civil Liberties (August 27, 2004).

<sup>13</sup> See Guidelines to Ensure that Information Privacy and other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (December, 2006).

<sup>14</sup> See Appendix 4, Addendum B to the *TSC MOU*.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

U//FOUO, without regard to the classification of the source material from which it is drawn. TERRORIST IDENTIFIERS include those listed in Addendum B (*i.e.*, names and aliases; dates of birth; places of birth; unique identifying numbers; passport information; countries of origin and nationality; physical identifiers; known locations; photographs or renderings; fingerprints or other biometric data; employment data; license plate numbers; and any other TERRORIST IDENTIFIERS that ORIGINATORS specifically provide for passage to the TSC). For example, email addresses and phone numbers are increasingly useful for screening purposes. ORIGINATORS should mark email addresses and phone numbers as U//FOUO whenever possible and pass these TERRORIST IDENTIFIERS to NCTC to forward to the TSC for inclusion in TSDB. ORIGINATORS are encouraged to provide all relevant and unclassified information, to include social media information when appropriate.

**III. CONSTITUTIONALLY PROTECTED ACTIVITIES**

**1.19 First Amendment.** First Amendment protected activity alone shall not be the basis for nominating an individual for inclusion on the Terrorist Watchlist.<sup>15</sup> The following are examples of protected Constitutional activities:

**1.19.1 Free Speech.** The exercise of free speech, guaranteed by the U.S. Constitution, includes more than simply speaking on a controversial topic in the town square. It includes such symbolic or other written, oral and expressive activities as carrying placards in a parade, sending letters to a newspaper editor, wearing a tee shirt with a political message, placing a bumper sticker critical of the President on one's car, and publishing books or articles. The common thread in these examples is conveying a public message or an idea through words or deeds. Speech that may be repugnant to ideas of the majority may still be protected by the U.S. Constitution. For the purpose of this Watchlisting Guidance, the right of protected free speech under the U.S. Constitution applies to U.S. PERSONS wherever they are located and to non- U.S. PERSONS located inside the United States. The right of protected free speech, however, is not unlimited and may not extend to some lawless action.

**1.19.2 Exercise of Religion.** The free exercise of religion covers any form of worship of a deity – even forms that are not widely known or practiced – as well as the right not to worship any deity. Protected religious exercise also extends to dress that is worn or food that is eaten for a religious purpose, attendance at a facility used for religious practice, observance of the Sabbath, raising money for evangelical or missionary purposes, and proselytizing.

**1.19.3 Freedom of the Press.** Freedom of the press includes such matters as reasonable access to news-making events, the making of documentaries, and the posting of "blogs."

---

<sup>15</sup> The First Amendment does not apply to non-U.S. PERSONS outside the United States. Before submitting nominations, NOMINATORS may consult with their Department or Agency counsel to determine whether a specific person is a U.S. PERSON and whether the questioned activity is entitled to First Amendment protection.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**1.19.4 Freedom of Peaceful Assembly.** Freedom of peaceful assembly, often called the right to freedom of association, includes gathering with others to protest government action, or to rally or demonstrate in favor of, or in opposition to, a social cause. The right to peaceful assembly includes more than just public demonstrations – it includes, as well, the posting of group websites on the Internet, recruiting others to a lawful cause, marketing a message, and fundraising, which all are protected First Amendment activities if they are conducted in support of an organizational, political, religious, or social cause.

**1.19.5 Petition the Government for Redress of Grievances.** The right to petition the government for redress of grievances includes, for example, writing letters to Congress, carrying a placard outside the city hall that delivers a political message, recruiting others to one's cause, and lobbying Congress or an Executive Agency for a particular result.

**1.20 Equal Protection.** The Equal Protection Clause of the U.S. Constitution provides in part that: "No State shall make or enforce any law which shall ... deny to any person within its jurisdiction the equal protection of the laws." The U.S. Supreme Court has made it clear that this applies as well to the official acts of U.S. Government personnel. Nominations, therefore, shall not be based solely on race, ethnicity, national origin, or religious affiliation. Any activities relating to this Guidance that are based solely on such considerations are invidious by definition, and therefore, unconstitutional.

## IV. WATCHLISTING POLICIES

**1.21 Watchlisting Disclosures.** The general policy of the U.S. Government is to neither confirm nor deny an individual's watchlist status. In addition to the provisions in Addendum B to the *TSC MOU*, which require NOMINATOR approval before TSDB information can be used in any process that might result in public disclosure, the 2007 *Memorandum of Understanding on Terrorist Watchlist Redress Procedures (Redress MOU)*<sup>16</sup> requires SCREENERS to contact the TSC if it receives a request for information or records that might reveal an individual's watchlist status. Approval would also be required from any entity which provided information used by a NOMINATOR during a nomination. Per the *Redress MOU*, ORIGINATING and NOMINATING AGENCIES are obligated to support SCREENER determinations – both at the administrative level and in litigation – and provide appropriate information, including unclassified substitutes as necessary. TSC, in conjunction with NCTC, the NOMINATORS, and the Department of Justice (DOJ), as appropriate, will ensure that representations regarding an individual's potential watchlist status are properly coordinated and approved.

**1.22 Legal or Use Restrictions.** Because information in the TSDB comes overwhelmingly from intelligence sources and methods or sensitive law enforcement techniques, Paragraph 12 of

---

<sup>16</sup> See Appendix 8, *Redress MOU*.



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

Addendum B to the *TSC MOU*<sup>17</sup> requires that any recipient of information from the TSDB seeking to use TERRORIST identity information in any legal or administrative process or proceeding obtain NOMINATOR approval before doing so. Approval from the entity which provided the information, if other than the NOMINATOR, is also required. Additionally, information from Foreign Intelligence Surveillance Act (FISA) collections may only be used in a proceeding with the advance authorization of the Attorney General. Therefore, any SCREENER seeking to use TSDB information in any process or proceeding must contact TSC so that TSC can assist in obtaining approval from the NOMINATOR, owner of the information, or Attorney General, as required.

- 1.23 In addition to the foregoing restrictions, there are restrictions on sharing information with foreign governments. Any TERRORIST IDENTIFIER (as described in Addendum B to the *TSC MOU*) will be deemed U//FOUO and shared with the watchlisting community and foreign governments for watchlisting purposes pursuant to the terms of the *TSC MOU*. Accordingly, NOMINATORS should include, as appropriate, TERRORIST IDENTIFIERS in documents that contain non-releasable warnings (*e.g.*, a report is not releasable to xxx/yyy/zzz countries), unless the TERRORIST IDENTIFIERS are restricted by some other authority that limits dissemination. If U.S. PERSON information is otherwise authorized for release to the foreign government, the non-releasable warning is disabled to allow dissemination of the information.

**V. WATCHLISTING STANDARD: IDENTIFYING AND SUBSTANTIVE DEROGATORY CRITERIA**

- 1.24 Before a KNOWN or SUSPECTED TERRORIST is added to the Terrorist Watchlist, TSC reviews the nomination to determine whether it meets the following minimum identifying criteria and minimum substantive derogatory criteria for inclusion in the TSDB.

1.24.1 **Minimum Identifying Criteria.** Each nomination must contain minimum identifying criteria for inclusion into the TSDB. Without this minimum identifying data, the nomination is not eligible for inclusion into the TSDB, or any of the TSC's supported systems. Chapter 2 sets forth guidance regarding both the minimum identifying biometric and biographic criteria for inclusion into the TSDB. Although TIDE accepts records containing less than these minimum criteria, such records will not be exported either to the TSDB for watchlisting or to the various supported systems used by the SCREENERS absent an exception described in the Watchlisting Guidance.

1.24.2 **Minimum Substantive Derogatory Criteria.** In addition to the minimum identifying criteria, nominations to the TSDB are accepted based on a REASONABLE SUSPICION that the individual is a KNOWN or SUSPECTED TERRORIST derived from the

---

<sup>17</sup> See Appendix 4, Addendum B to the *TSC MOU*.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

totality of the information reviewed for nomination.<sup>18</sup> To demonstrate that the nomination has sufficient indicia of reliability to support this REASONABLE SUSPICION determination, NOMINATING AGENCIES should implement processes designed to ensure that nominations are free from errors, that recalled or revised information is reviewed regularly, and that necessary corrections to nominations based on those revisions/retractions are made. NOMINATING AGENCIES should, to the extent possible given the nature of the reporting, verify the accuracy and reliability of the information included in nominations. In some cases, the NOMINATING AGENCY may not be able to evaluate the reliability of the information received; however, in such situations, the NOMINATING AGENCY can ensure that the information provided is an accurate representation of the information obtained. Chapter 3 sets forth further guidance regarding the application of the REASONABLE SUSPICION standard to TSDB nominations.

**VI. WATCHLISTING PROCESS OVERVIEW**

- 1.25 The authorities referenced in Section II of this Chapter created the framework for the watchlisting enterprise by combining various functions of existing government entities and joining them to new organizations with counterterrorism responsibilities. The resulting watchlisting enterprise consists of ORIGINATORS, NOMINATORS, AGGREGATORS, SCREENERS and encountering agencies that are supported by the community-wide collection, nomination, and consolidation processes.
- 1.26 **ORIGINATORS, NOMINATORS, AGGREGATORS, and SCREENERS.** All Executive Departments and Agencies have responsibility for collecting, collating, and sharing TERRORISM INFORMATION to support the watchlisting process. They are called ORIGINATORS because they initially collect and identify information supporting the conclusion that an individual is a KNOWN or SUSPECTED TERRORIST. An ORIGINATOR is the Department or Agency that has appropriate subject matter interest and classification authority and collects TERRORISM INFORMATION (*i.e.*, raw information) and disseminates it or TERRORIST IDENTIFIERS to other U.S. Government entities via an intelligence report (*i.e.*, finished intelligence) or other mechanism. In general, when an ORIGINATOR has identified international TERRORISM INFORMATION and determines that information should be provided to NCTC, the ORIGINATOR takes on the NOMINATOR role. A NOMINATOR is a Federal Department or Agency that has information to indicate that an individual meets the criteria for a KNOWN or SUSPECTED TERRORIST and nominates that individual to TIDE and the TSDB based on information that originated with that Agency.
- 1.27 While all NOMINATORS have the duty of upholding informational standards, the NCTC and TSC are distinctly responsible for ensuring data quality and the integrity of their respective repositories. NCTC and TSC are themselves potential NOMINATORS. Analysts from the

---

<sup>18</sup> Please note that there are also certain exceptions to the minimum biographic information and minimum substantive derogatory criteria required for Terrorist Watchlist nominations that support immigration and visa screening activities conducted by DHS and DOS. See Chapter 2, Section III and Chapter 3, Section V.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

NCTC may discover an individual who is eligible for watchlisting while reviewing all-source information. In these cases, NCTC analysts will request that the ORIGINATOR submit a nomination for inclusion into TIDE; or, on a limited basis or during exigent circumstances, NCTC analysts may update TIDE directly with a disseminated report and notice to the ORIGINATOR(S). In instances where disseminated reporting is used to enhance TIDE, NCTC will provide notice back to the collecting agency via TIDE. TSC may also nominate TERRORISM INFORMATION received pursuant to TERRORISM screening conducted by foreign governments.

- 1.28 NCTC and TSC are responsible for reviewing both newly nominated individuals, as well as subsets of existing records, to determine if additional and/or enhancement (research) is required to locate missing information critical to the watchlisting process. In some cases, this will require research to locate additional DEROGATORY INFORMATION to meet the minimum substantive derogatory criteria for watchlisting. In other cases, this will require research to locate additional biographic or biometric identifiers, in order to provide a comprehensive record maximizing the probability of confirming a POSITIVE MATCH to an identity contained in the TSDB.
- 1.29 AGGREGATORS are those who receive and hold TERRORISM INFORMATION and certain other non-TERRORISM INFORMATION they are authorized to receive and retain. For example, two of NCTC's main statutory missions are to serve as the (1) central and shared knowledge bank on KNOWN or SUSPECTED TERRORISTS and (2) primary organization in the U.S. Government for analyzing and integrating all intelligence information possessed or acquired by the U.S. Government pertaining to TERRORISM and counterterrorism.<sup>19</sup>
- 1.30 TSC takes on the role of an AGGREGATOR when a KNOWN or SUSPECTED TERRORIST is encountered and the individual's record is enhanced or updated with ENCOUNTER-related information. As noted in Paragraphs 1.1 and 1.7, the TSC manages the watchlisting process and plays a key role in helping Departments and Agencies determine whether an ENCOUNTER with a member of the public is one with a KNOWN or SUSPECTED TERRORIST. Additional TERRORISM INFORMATION or TERRORIST IDENTIFIERS are generated during ENCOUNTERS and the Encounter Management Application (EMA)<sup>20</sup> uses that information to update records of KNOWN or SUSPECTED TERRORISTS.
- 1.31 SCREENERS vet against the TSDB to determine if an individual is a possible match to a KNOWN or SUSPECTED TERRORIST in the TSDB. SCREENERS can include federal, state, local, tribal, territorial, or foreign governments and certain private entities. Screening officials include homeland security officers, consular affairs officers, transportation safety personnel, and officials of foreign governments with whom the United States has entered into a TERRORISM SCREENING INFORMATION sharing agreement pursuant to HSPD-6. Certain Departments and Agencies have components which perform both screening and law enforcement duties. If a

<sup>19</sup> See 50 U.S.C. §404o.

<sup>20</sup> EMA is an application used by the TSC to administer ENCOUNTER information.

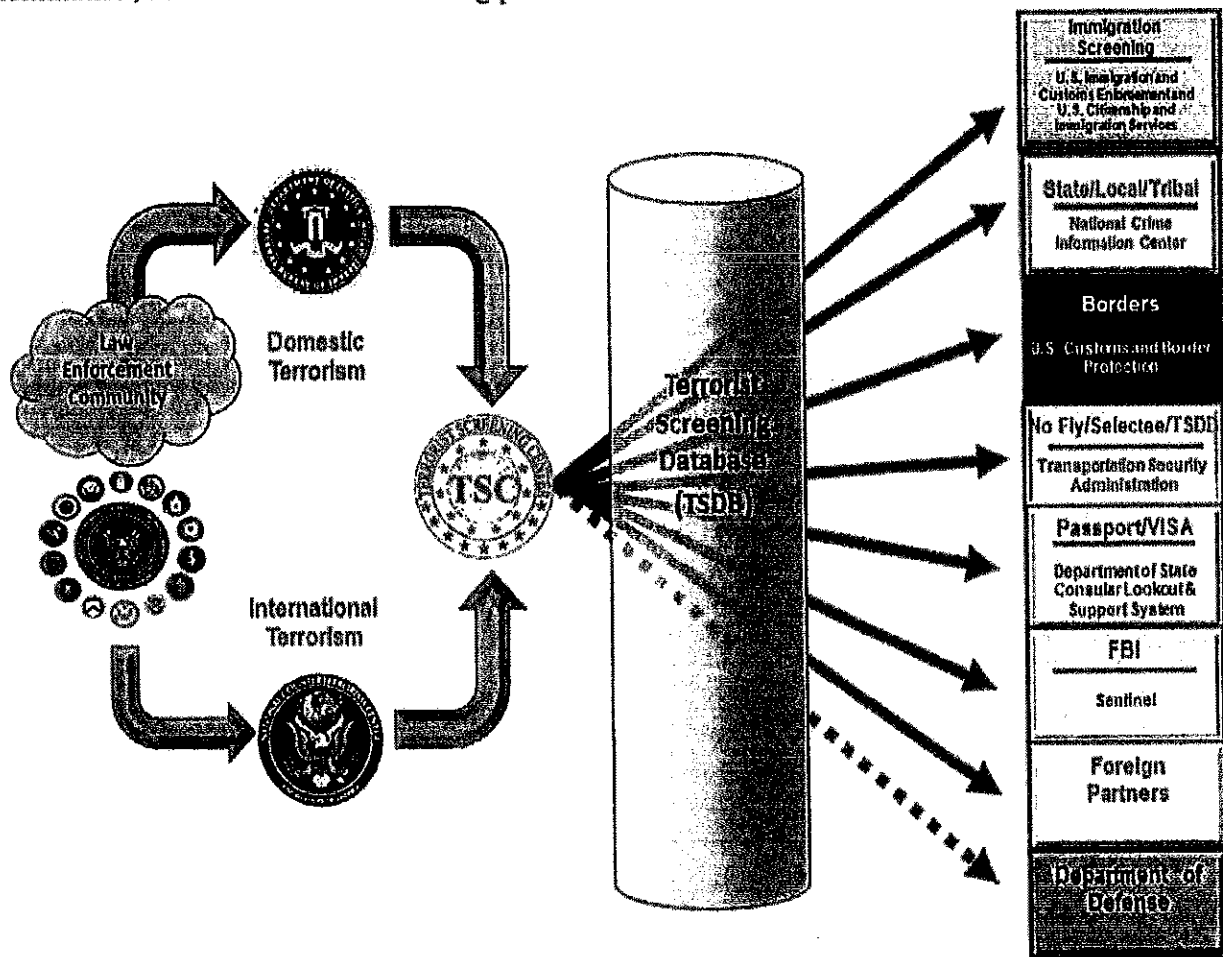
**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

SCREENER believes an individual may be on the Watchlist, the screener contacts the TSC's Terrorist Screening Operations Center (TSOC). The TSOC will determine whether the individual the SCREENER has encountered is, in fact, a POSITIVE MATCH to the individual who is on the Terrorist Watchlist. The TSOC may also notify the FBI's Counterterrorism Division (CTD) that there has been a positive ENCOUNTER with a watchlisted subject. TSC's Terrorist Screening Operations Unit (TSOU) coordinates the appropriate operational response to the ENCOUNTER. Based on the TERRORISM INFORMATION made available by the ORIGINATING AGENCY, the SCREENER will take action based upon its specific authorities (e.g., requiring additional screening at an airport checkpoint, denying a visa application, determining admissibility into the United States) and follow appropriate ENCOUNTER procedures, as set forth in Chapter 5.

- 1.32 **Collection, Nomination, Consolidation and the Use of the Terrorist Watchlist to Perform Screening Processes.** The following is a chart depicting the collection, TERRORIST nomination, consolidation and screening processes:



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 1.33 The arrows fade inside the TSDB cylinder because not every nomination from NCTC (for international TERRORISM) or the FBI (for domestic TERRORISM) is exported from the TSDB to SCREENERS (represented by the multi-colored blocks at the far right of the chart).<sup>21</sup> For example, certain categories of individuals that do not meet the minimum identifying criteria (see Chapter 2, Section II) or the REASONABLE SUSPICION standard (see Chapter 3, Section II) can be watchlisted to support immigration and visa screening activities by DHS and DOS (see Chapter 3, Section V) but are not exported to state/local/tribal SCREENERS or foreign partners. Similarly, when ORIGINATORS provide FRAGMENTARY INFORMATION to NCTC for inclusion in TIDE, such information will not be exported from TIDE to the TSDB, unless the NOMINATING AGENCY believes there is REASONABLE SUSPICION to believe that the individual is a KNOWN or SUSPECTED TERRORIST. FRAGMENTARY INFORMATION is provided to NCTC where it can be further analyzed, connected to existing information, and added to TIDE for export to TSDB because NCTC, and not individual ORIGINATORS, has access to all the information available to the U.S. Government on a KNOWN or SUSPECTED TERRORIST.

## **VII. ROLES AND RESPONSIBILITIES FOR THE WATCHLISTING AND SCREENING COMMUNITY**

- 1.34 Delineation of roles and responsibilities of NOMINATING AGENCIES, SCREENERS, NCTC, and the TSC is critical to provide for an effective and efficient integrated Terrorist Watchlist enterprise. While HSPD-6 describes the broad mandate of developing an integrated watchlist system, and the *TSC MOU* provides a level of detail needed to fulfill that mandate, further clarification is required to ensure there are neither gaps in the nomination process, nor wasteful redundancies.
- 1.35 Pursuant to HSPD-6, Departments and Agencies in the Executive Branch are required, to the extent permitted by law, to provide TERRORIST INFORMATION to NCTC. This process will be accomplished either through direct nomination to NCTC, or through a specific component designated by a Federal Department or Agency head for doing so (e.g., all DOJ components are directed to nominate through the FBI; DHS Intelligence and Analysis (I&A) has oversight responsibility for all DHS nominations). Except as detailed in the sections applicable to expedited nominations (see Paragraphs 1.58 and 1.59), NOMINATING AGENCIES will endeavor to provide comprehensive nominations and include the maximum amount of identifying and DEROGATORY INFORMATION.<sup>22</sup> NOMINATING DEPARTMENTS AND AGENCIES should prioritize

<sup>21</sup> The Terrorist Screening Database Annex D to the FBI Memorandum of Understanding with Department of Defense (DoD), signed February 22, 2012, established DoD as a screening agency customer of the TSC. The dashed line in the latter chart represents that DoD is finalizing procedures to receive and use information from the TSDB for its screening processes.

<sup>22</sup> In May 2010, the Deputies asked that NOMINATING AGENCIES "ensure that nominations are comprehensive and include the maximum amount of identifying and DEROGATORY INFORMATION." In 2012, the Interagency Policy Committee (IPC), in coordination with NOMINATORS, SCREENERS, NCTC and TSC, developed a prioritized list of data identifiers that are critical to screening and identity resolution activities. This *Identity Resolution and Enhancement Tiers* document is available on NCTC's Watchlisting Community of Interest portal on the Joint Worldwide Intelligence Communications System (JWICS).

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

the identification of new KNOWN or SUSPECTED TERRORISTS who meet the REASONABLE SUSPICION standard, along with the identifying and DEROGATORY INFORMATION most useful to watchlisting, and screening effort, as well as assisting in identity resolution.

- 1.36 Each Department or Agency that nominates a KNOWN or SUSPECTED TERRORIST to NCTC for watchlisting is under a continuing obligation to provide NCTC with newly identified DEROGATORY INFORMATION or exculpatory information obtained by that Department or Agency. Each Department or Agency also has the responsibility to provide NCTC with newly identified identifying and DEROGATORY INFORMATION obtained from their Department or Agency, regardless if they were the original NOMINATING AGENCY.
- 1.37 With the noted exception of the Visa Viper Program, Departments and Agencies should not nominate KNOWN or SUSPECTED TERRORISTS to NCTC based on information that they do not originate without first coordinating with the ORIGINATOR.

**VIII. QUALITY CONTROL MEASURES**

- 1.38 In order to produce and maintain the most reliable and accurate information in TIDE, TSDB, and screening databases, quality control is considered a responsibility of all entities. NOMINATING DEPARTMENTS AND AGENCIES must establish and maintain processes, including appropriate training and guidance, to ensure information transmitted to NCTC is consistent with the source of the information.
- 1.39 **HSPD-6 Requirements.** HSPD-6 requires the TSC to maintain thorough, accurate, and current information concerning KNOWN or SUSPECTED TERRORISTS. For watchlisting purposes, "current" means information that the NOMINATING AGENCY reasonably believes is valid and accurate. The requirement that information be current does not necessarily preclude information that is several years old from being included in the TSDB if there is no reason to believe the information may have changed (*e.g.*, information regarding an individual's date of birth or TERRORIST ACTIVITY was collected 20 years ago but has not been superseded by additional information is still relevant). NOMINATORS should consider the date of the DEROGATORY INFORMATION in the context of analyzing the overall quality of the data, as well as the severity of the threat, to determine whether the individual warrants watchlisting. The date of the DEROGATORY INFORMATION may refer to both the date the information is collected (such as a report that was collected 50 years ago) as well as the date of the information that is referenced in the reporting (such as a recent report that references an event that occurred 50 years ago).
- 1.40 **TSC MOU Obligations.** Paragraph 15 of the *TSC MOU* provides that the TSC "will determine, according to criteria established jointly with the entity responsible for each supported system, which supported screening processes will query that entry in the consolidated TERRORIST screening database." Pursuant to that paragraph, the TSC is required to "make these determinations based on criteria and procedures developed in coordination with the Parties to this Memorandum and in consultation with the heads of appropriate Federal

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

Departments and Agencies based on factors, including but not limited to, the following:

- 1.40.1 the nature of the person's association with TERRORISM;
- 1.40.2 the quality of the data, including credibility, reliability, and extent of corroboration; and,
- 1.40.3 the extent of uniquely identifying data. . . ."<sup>23</sup>

- 1.41 **Provide Guidance and Training.** Each Agency will provide guidance on the watchlisting business process. Analysts will receive periodic refresher training, as needed.
- 1.42 **NOMINATING AGENCY Procedures.** Each NOMINATOR providing international TERRORIST watchlisting nominations to NCTC is responsible for the accuracy of its information and has a continuing responsibility to notify NCTC of any changes that affect the validity or reliability of such information.<sup>24</sup> NCTC analysts will review each nomination for TERRORIST watchlisting prior to its inclusion into TIDE and its export to the TSDB.
- 1.43 Each NOMINATING AGENCY should implement processes designed to ensure that nominations are free from errors, that recalled or revised information is reviewed regularly, and that necessary corrections to nominations based on those revisions/retractions are made. NOMINATING AGENCIES should, to the extent possible given the nature of the reporting, verify the accuracy and reliability of the information included in nominations. The following represents the type of processes that each NOMINATING AGENCY shall develop that are tailored to each Agency's particular mission and operational environment:
  - 1.43.1 **Develop Adequate Factual Predicate.** Each NOMINATING AGENCY will seek to obtain as much DEROGATORY INFORMATION and identifying information as practicable concerning the KNOWN or SUSPECTED TERRORIST who is being nominated.
  - 1.43.2 **Provide Guidance and Training.** Each NOMINATING AGENCY will provide guidance on the TERRORIST watchlisting nomination process and ensure that analysts involved in the nomination process are trained on a periodic basis.
  - 1.43.3 **Require Quality Assurance Review.** Each NOMINATING AGENCY will use a quality assurance process to review nominations for accuracy prior to forwarding the information to NCTC.
  - 1.43.4 **Heightened Review for U.S. PERSONS.** The nominations of U.S. PERSONS require

---

<sup>23</sup> See Appendix 3, *TSC MOU*.

<sup>24</sup> PURELY DOMESTIC TERRORISM INFORMATION is provided directly to TSC by the FBI and is subject to the same conditions applicable to the nomination procedures for those associated with international TERRORISM.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

special considerations and procedures.<sup>25</sup> See Paragraph 3.15.

- 1.43.5 **U.S. PERSON Determinations.** NOMINATORS must take reasonable steps to determine whether an individual is a U.S. PERSON.
- 1.43.6 **U.S. PERSON Review and Confirmation.** Nominations of U.S. PERSONS to the Terrorist Watchlist shall be reviewed by the NOMINATING AGENCY'S legal counsel or a designated reviewer to confirm that the REASONABLE SUSPICION standard has been met or that the nomination meets an exception to the REASONABLE SUSPICION standard, and to ensure that the nomination conforms to Agency specific U.S. PERSON authorities and guidelines.
- 1.43.7 **Reliability and Accuracy Limitations.** Nominations will include any limitations on the reliability or accuracy of the information.
- 1.43.8 **Periodic Reviews.** The NOMINATING AGENCY will conduct periodic reviews of their nominations of U.S. PERSONS to the Terrorist Watchlist, at minimum on an annual basis, when there is no corresponding FBI investigation to ensure that the U.S. PERSON continues to meet watchlisting criteria.
- 1.43.9 **Redress Procedures.** As per the establishment of a formal watchlist redress process (see Chapter 1, Section XI), entities involved in the watchlisting process shall establish internal reviews and redress procedures.
- 1.44 Each NOMINATING AGENCY will have procedures that facilitate the prevention, identification, and correction of any errors in information that is shared as part of the watchlisting process. Procedures will include the review of retractions and/or corrections of information that may have been used to support a nomination. In cases where a retraction or other information has become available, the NOMINATING AGENCY will promptly send a watchlist removal request or modification, as appropriate, to NCTC. Each NOMINATING AGENCY must provide notice of any errors or outdated information to NCTC immediately unless there is an articulated reason why such notification could not be made immediately. NCTC will process and transmit to TSC such corrections upon receipt.
- 1.45 **NCTC Review.** In addition to review by NCTC analysts, NCTC will employ a quality control process to ensure that all standards and appropriate procedures have been employed, the data is accurate, and the presentation of the material is clear, concise, and complies with established definitions and conventions. NCTC must also have processes and procedures in place to ensure the information documented in TIDE and provided to the TSC is accurately transcribed. NCTC shall ensure there is a process in place for review and/or auditing of TIDE records.

---

<sup>25</sup> See Executive Order 12333, as amended, and 5 U.S.C. 552a(e)(7).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 1.46 **TSC Review.** TSC personnel will review the nominations received as described in Paragraph 1.56. TSC personnel evaluate whether nominations meet watchlisting standards and weigh, as appropriate, all-source analysis before accepting or rejecting a nomination. The TSC has a critical role to play in quality control, as the TSC review is the last step before any record (including a biometric nomination where no name is available) is sent to various screening systems. As with NCTC, the TSC should ensure there is a process in place for review and/or auditing of TSC nominations and TSC records.

**IX. NOMINATION PROCEDURES**

- 1.47 **Distinctions between U.S. PERSONS under Executive Order 12333 and Aliens under the Immigration and Nationality Act.** This Watchlisting Guidance generally adopts the definition of U.S. PERSON from Executive Order 12333 (as amended) for nomination procedures. Executive Order 12333 defines a U.S. PERSON as "A United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed or controlled by a foreign government or governments." The Watchlisting Guidance also contains certain exceptions to the minimum substantive derogatory standards for TERRORIST watchlisting that support immigration and visa screening activities by the DHS and DOS to determine whether ineligibilities exist for admission to the United States or visa adjudication pursuant to the Immigration and Nationality Act (INA). Because the INA defines "aliens" as any person not a citizen or national of the United States, the INA admissibility provisions also apply to Lawful Permanent Residents (LPRs), in certain circumstances, who are considered U.S. PERSONS under Executive Order 12333. Consequently, NCTC developed a mechanism in TIDE to identify and distinguish U.S. citizens from non-U.S. citizens in order to further distinguish between "aliens" under the INA and U.S. PERSONS under Executive Order 12333.<sup>26</sup>
- 1.48 **ORIGINATOR's Nominations Procedures.** As mentioned in Paragraph 1.26, when an ORIGINATOR becomes a NOMINATOR, it prepares a nomination document and forwards it to NCTC through the NOMINATOR tool.
- 1.48.1 As a general rule, NCTC will attach all disseminated communications (cables or forms) to the TERRORIST identities record as a "source" document, which will be available on NCTC Current or the Joint Worldwide Intelligence Communications System (JWICS) to individuals who have been granted access to TIDE.
- 1.48.2 Because NCTC is the conduit for passing international TERRORISM INFORMATION to TSC for TERRORISM screening purposes, there is no longer a need to send watchlist requests to multiple Government Agencies. By sending a Terrorist Watchlist nomination cable to NCTC, all potential U.S. Government TERRORISM screening

---

<sup>26</sup> See INA § 101(a)(3) [8 U.S.C. 1101(a)(3)].

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

responsibilities should be accounted for.

1.48.3 The DOJ has approved a Protocol to govern TERRORIST nominations for its non-FBI components, which requires components to provide the FBI with all TERRORISM INFORMATION.<sup>27</sup> The FBI is responsible for submitting watchlisting nominations based on information received from other DOJ components pursuant to the FBI's nomination procedures.

1.48.4 DHS has designated the Under Secretary for I&A as the Executive Agent for DHS' centralized TERRORIST watchlisting process and he/she shall be responsible for providing a DHS wide-mechanism for nominating all identifying or DEROGATORY INFORMATION about KNOWN or SUSPECTED TERRORISTS to TIDE. DHS I&A is also responsible for providing training/certification programs to the components.

1.49 In providing information to NCTC for inclusion into TIDE, the ORIGINATOR is responsible for determining whether it may, by law, provide the information to NCTC, in accordance with section 1021(d)(6) of IRTPA. This information shall be provided with any applicable caveats or dissemination controls, which will be reflected in TIDE. The biographic and biometric identifiers derived from this information will be deemed U//FOUO for passage to TSDB unless the ORIGINATOR designates them as "TIDE Restricted," as outlined in Addendum B to the *TSC MOU*.

1.50 **NCTC Actions and Processes.** NCTC reviews TERRORIST nominations from Federal Departments or Agencies (NOMINATORS) as described in Paragraph 1.28.

1.51 In determining whether an individual is a KNOWN or SUSPECTED TERRORIST, NCTC will rely on the designation of "KNOWN TERRORIST" provided by the NOMINATOR as presumptively valid. This presumption can be overcome if NCTC has specific and credible information within its possession that such designation is not appropriate, at which point NCTC will provide such information to the NOMINATOR.

1.52 In reviewing whether to include the TERRORISM INFORMATION about the KNOWN or SUSPECTED TERRORIST in TIDE, NCTC reviews the totality of information. The totality of information is evaluated based on the experience of the reviewer, and the facts and rational inferences that may be drawn from those facts, including past conduct, current actions, and credible intelligence concerning future conduct. As part of this review, NCTC will determine if the information pertains to, or is related to, TERRORISM. TIDE includes TERRORISM INFORMATION on KNOWN or SUSPECTED TERRORISTS and may include additional TERRORISM INFORMATION beyond what meets the minimum substantive derogatory and identifying criteria required for nominations to the TSDB, as described in Paragraph 1.24. Upon conclusion of NCTC's review, NCTC will either accept or reject the nomination:

---

<sup>27</sup> See Appendix 7, DOJ Protocol on Terrorist Nominations.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**1.52.1 Accept Nomination.** If a nomination contains TERRORISM INFORMATION, NCTC will create or enhance the associated TIDE record with the data contained in the nomination. If the minimum substantive derogatory and identifying criteria are met, NCTC will forward the TERRORIST IDENTIFIERS to the TSC for placement in TSDB with the NOMINATOR'S watchlist recommendation.

**1.52.2 Reject Nomination.** If a nomination does not contain TERRORISM INFORMATION, NCTC may reject the nomination. NCTC will review rejected nominations and search holdings for additional data that may support a TERRORISM INFORMATION finding. If no information is found to support the nomination, NCTC will notify the NOMINATING AGENCY of the rejection.

**1.53 Types of records in TIDE.** There are two types of records in TIDE:

**1.53.1 TERRORIST Records.** The vast majority of records in TIDE are for KNOWN or SUSPECTED international TERRORISTS. These records are labeled "TERRORISTS." Only a small percentage of TERRORIST records in TIDE concern U.S. PERSONS.

**1.53.2 Non-TERRORIST Records.** A small percentage of records in TIDE are identified and labeled "Non-TERRORISTS."<sup>28</sup> These records are generally of familial family members or associates of KNOWN or SUSPECTED TERRORISTS and assist DOS and DHS in, for example, adjudicating visas and immigration processing, or assist the IC in tracking KNOWN TERRORISTS. These "Non-TERRORISTS" include:

**1.53.2.1 Alien Spouses and Children of TERRORISTS.** Based on section 212(a)(3)(B)(i)(IX) of the INA, alien spouses and children of TERRORISTS may be inadmissible to the United States.<sup>29</sup> TIDE exports records pertaining to alien spouses and children of alien international TERRORISTS (also known as TIDE Category Code 17) to support immigration and visa screening activities by DOS and DHS;

**1.53.2.2 Other Relatives.** TIDE also includes "non-TERRORIST" records of individuals who have a close relationship to a KNOWN or SUSPECTED international

<sup>28</sup> TIDE records for non-U.S. citizens, including LPRs, with insufficient DEROGATORY INFORMATION to meet the REASONABLE SUSPICION standard (TIDE Category Code 99) and records relating to an individual who has a defined relationship with the KNOWN or SUSPECTED TERRORIST, but whose involvement with the KNOWN or SUSPECTED TERRORIST'S activities is unknown (TIDE Category Code 50) are exported to the TSDB as TSDB exceptions to the REASONABLE SUSPICION standard. Additionally, individuals described by sources as "TERRORISTS", "extremists", "jihadists", "militants", "mujahideen" or "insurgents" (TIDE Category Code 03, also referred to as a "labels plus" nomination) will be accepted into the TSDB as exceptions for export to DHS and DOS for immigration and border processing. See Paragraph 3.14.6. A complete list of TIDE Category Codes can found under the "Watchlisting Criteria Guidance" section on the Intelink website at <http://www.intelink.gov/tsc/legal.htm>.

<sup>29</sup> "Any alien who. . . is the spouse or child of an alien who is inadmissible under this subparagraph, if the activity causing the alien to be found inadmissible occurred within the last 5 years, is inadmissible." See INA § 212(a)(3)(B)(i)(IX) [8 U.S.C. 1182(a)(3)(B)(i)(IX)].

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

TERRORIST but are not alien spouses or children of a TERRORIST. For instance, the father or brother of a TERRORIST could have a record in TIDE (also known as TIDE Category Code 160). Thus, these "other relatives" could be U.S. PERSONS or non-U.S. PERSONS. Identifiers for these other relations reside in TIDE but are not exported to the TSC for watchlisting, absent independent DEROGATORY INFORMATION. Instead, these records may be retained in TIDE for analytic purposes;

1.53.2.3 **Passports.** Unrecovered lost or stolen passports in the hands of international TERRORISTS (also known as TIDE Category Code 89);

1.53.2.4 **Associates.** Individuals who have a defined relationship with the KNOWN or SUSPECTED TERRORIST, but whose involvement with the KNOWN or SUSPECTED TERRORIST's activities is unknown (also known as TIDE Category Code 50);

1.53.2.5 **Individuals with a Possible Nexus to TERRORISM.** Individuals with a possible nexus to TERRORISM and/or TERRORIST ACTIVITY but for whom additional DEROGATORY INFORMATION is needed to meet the REASONABLE SUSPICION standard (also known as TIDE Category Code 99).

1.54 **Identification of U.S. PERSON Status in TIDE.** NCTC analysts will review the totality of information available on a subject to discern U.S. PERSON status prior to creating or enhancing a record in TIDE, whenever possible. For existing TIDE records, this status is available to the analyst in the first field of the TIDE record. In case of external nominations or ENHANCEMENTS from the IC, the standard nomination template provides a means for NOMINATORS to identify U.S. PERSON status pursuant to Executive Order 12333 and the Agency's specific guidelines. The U.S. PERSON status field on the standard nomination template is a required field and it is the responsibility of each NOMINATING AGENCY to ensure the field is properly annotated in accordance with established policy.

1.55 **Types of Records in TIDE and the TSDB.** Not all records in TIDE are included in the TSDB. For example, records with FRAGMENTARY INFORMATION that do not meet the minimum derogatory standard or records that do not meet identifying information criteria remain in TIDE and are not included in the TSDB, absent direction for temporary, threat based categories pursuant to Paragraph 1.59.<sup>30</sup> The nominations process for TIDE records that will be considered for entry in the TSDB begins with an automated data transfer process that moves an individual TIDE record containing the identity of a KNOWN or SUSPECTED TERRORIST or other exportable category or record nominated for watchlisting to the TSDB.

1.56 **TSC Actions and Processes.** The TSC's Single Review Queue (SRQ) enables the TSC's Nominations and Data Integrity Unit (NDIU) to review each KNOWN or SUSPECTED TERRORIST

---

<sup>30</sup> Certain categories of non-TERRORIST records (see Paragraph 1.53.2) or nominations to the No Fly and Selectee List based on an expedited waiver of "full date of birth" requirement (see Paragraph 4.18) may also be eligible for inclusion in the TSDB.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

record nomination to ensure it meets the watchlisting standard.<sup>31</sup> The SRQ also helps ensure that all qualified records are made available to the appropriate SCREENERS for use in TERRORISM screening. During the SRQ process, every request to add, modify, or delete a TSDB record is reviewed by a TSC analyst to ensure the accuracy of watchlisting records and the removal of inaccurate records from TSDB.

1.56.1 Within the TSC's NDIU, experienced analysts and/or designated Agency representatives serve as Subject Matter Experts (SMEs) with respect to specific databases (e.g., No Fly or Selectee List) that receive TSDB data for TERRORISM screening purposes. The NDIU currently has four types of SMEs who specialize in the information/systems from their respective organizations: DHS/Transportation Security Administration (TSA) for the No Fly, Selectee and Expanded Selectee Lists, FBI for National Crime Information Center (NCIC)/KNOWN or SUSPECTED TERRORIST File (KSTF), DOS for the Consular Consolidated Database (CCD)<sup>32</sup> and DHS for TECS (and its components) and the Automated Targeting System (ATS). SMEs provide guidance regarding their specific information/systems to the TSC and watchlisting standards to their Agencies. In some cases, the SME coordinates the data export to the supported system, provides feedback to NOMINATORS, and responds to inquiries regarding their supported system from other TSC customer Agencies.

1.56.2 Upon the conclusion of TSC's review, TSC will either accept or reject the nomination:

1.56.2.1 **Accept Nomination.** Consistent with Paragraphs (7) and (8) of Addendum B to the *TSC MOU*, if a nomination contains the minimum substantive derogatory criteria and the minimum identifying information, TSC will create a TSDB record, include the TERRORIST IDENTIFIERS from the TIDE record, and export the TSDB record to its supported systems (i.e., databases and systems eligible to receive records from the TSDB) for the benefit of SCREENERS that conduct TERRORISM screening. The current supported systems include, but are not limited to, the following:

- 1.56.2.1.1 NCIC/KSTF;
- 1.56.2.1.2 DOS Consular Lookout and Support System (CLASS)-VISA and CCD;
- 1.56.2.1.3 DHS Watchlisting Service (WLS) (e.g., TECS, ATS, Secure Flight);
- 1.56.2.1.4 TSA Transportation Security Vetting Center;
- 1.56.2.1.5 TSA-Office of Intelligence Analysis (OIA);
- 1.56.2.1.6 Tipoff United States Canada (TUSCAN);

<sup>31</sup> See Chapter I, Section VIII, *supra*.

<sup>32</sup> CCD is an application used by DOS to administer its visa and passport applications.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## 1.56.2.1.7 Tipoff Australia Counterterrorism Information Control System (TACTICS).

1.56.2.2 **Reject Nomination.** If a nomination lacks either the minimum substantive derogatory criteria or the minimum identifying information, and is not an exception to those requirements (e.g., TIDE Category Codes 50 or 99 as described in Paragraph 1.53.2), TSC will reject the nomination and notify NCTC directly of its determination or coordinate with NCTC to notify the NOMINATOR of its determination. Records nominated to TIDE that are ineligible for TERRORIST watchlisting may remain in TIDE until additional information is obtained to warrant either watchlisting or removal from TIDE. NCTC analysts will review all-source information for additional identifying or substantive DEROGATORY INFORMATION. If additional information is discovered, NCTC will enhance the TIDE record and submit the record to TSC for inclusion in the TSDB. The TIDE record will be reviewed again by the TSC to determine whether it is eligible for watchlisting in TSDB and export to certain supported screening systems.<sup>33</sup>

1.57 The number of TSC's supported systems will continue to grow as TSC, DHS, and DOS expand their domestic and international outreach efforts and finalize additional agreements to exchange TERRORISM SCREENING INFORMATION. TSC has modified the TSDB so that certain customers may query the TSDB remotely instead of receiving exports of TSDB data to their own systems.

1.58 **Expedited Nomination Procedures for Individual Nominations.** If exigent circumstances exist (imminent travel and/or threat) where an individual nomination into the TSDB needs to be expedited after normal duty hours, a NOMINATOR, with coordination from NCTC, may contact the TSC's TSOC directly. If a NOMINATOR coordinated with NCTC, the nomination will be received by the TSC via the SRQ in TSDB and the TSOC Watch Commander will coordinate with a NDIU Senior Analyst to process the nomination. A NOMINATOR may also contact the TSC directly and provide all relevant information using the following process:

1.58.1 The NOMINATOR must first contact the TSOC at 866- [REDACTED] (toll free number) or at 571- [REDACTED].

1.58.2 The NOMINATOR will be instructed by a TSOC Specialist on how to telephonically complete a Terrorist Screening Center Expedited Nomination Request Form.

1.58.3 In addition to basic identifying information, the NOMINATOR will be requested to provide a 24/7 point of contact should the KNOWN or SUSPECTED TERRORIST be encountered by a SCREENER.

---

<sup>33</sup> See Paragraph 1.24.2 *supra*.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

1.58.4 Within 72 hours of contacting the TSOC, the NOMINATOR must provide appropriate follow-up documentation that articulates, through either classified or unclassified means, the substantive DEROGATORY INFORMATION used to establish the basis for TERRORIST watchlisting.

**1.59 Expedited Nomination Procedures for Temporary, Threat-Based Categories.** This provision is intended to enable categories of individuals to be temporarily upgraded in watchlist status based on current and credible intelligence information or a particular threat stream that indicates a certain category of individuals may be used to conduct an act of domestic or international TERRORISM. This temporary, threat-based expedited upgrade (TBU) is made at the direction of the Assistant to the President for Homeland Security and Counterterrorism or his/her designee (Appropriate Official) and should be narrowly tailored to address the threat.

1.59.1 The goal of this provision is to fashion a watchlisting response that is appropriate to the nature, specificity, and severity of the threat. To achieve this goal, in addition to verifying the credibility of the threat intelligence, due consideration should be given to:

1.59.1.1 The harm to public safety posed by the threat;

1.59.1.2 The clarity and specificity of the information giving rise to the threat as to time, place, method, and identity of the suspected perpetrators;

1.59.1.3 The anticipated impact on international and domestic travel, civil liberties, and foreign relations; and,

1.59.1.4 The best available screening tools, other than the No Fly or Selectee Lists, given the type and specificity of identifiers and travel data.

1.59.2 When necessitated by exigent circumstances, and where there is current and credible intelligence information or a particular threat stream that indicates a certain category of individuals may be used to conduct an act of domestic or international TERRORISM, the Appropriate Official may direct the TSC and NCTC to place categories of individuals from TIDE or TSDB on the No Fly List, Selectee List, or into the TSDB for up to 72 hours before concurrence is obtained from the Deputies or Principals Committee. To the extent practicable, the initial direction to NCTC and TSC from the Appropriate Official will be in writing. Absent DEROGATORY INFORMATION supporting individual nomination or watchlist upgrade, if written concurrence is not obtained within 72 hours of the initial direction to TSC and NCTC, the TSC will automatically remove any individuals added to the No Fly List, Selectee List, or TSDB pursuant to the TBU, until such written direction is received.

1.59.3 The addition of categories of individuals to the No Fly List, Selectee List, or TSDB pursuant to Paragraph 1.59.2 shall be effected for a period of time, consistent with the

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

nature of the threat involved, not to exceed 30 days but may be renewed for additional 30-day periods upon written approval of the Deputies or Principals Committee. A TBU is valid until the threat no longer exists. To the extent that such threat recedes or is otherwise mitigated prior to the expiration of 30 days or during any extension approved by the Deputies or Principals Committee, TSC and NCTC and members of the watchlisting community shall immediately request of the Deputies or Principals Committee to downgrade these TBUs to their original or appropriate status. All threat-based records transmitted through automated mechanisms (*i.e.*, WLS, CCD) will include a "TBU indicator" at the message level to differentiate this category of records from non-TBU records and to provide the TBU directive for which the record is upgraded.

1.59.4 Until such time as the Deputies or Principals provide additional, written guidance, DOS will defer visa actions with respect to these expedited upgrades in watchlist status.

1.59.5 Departments and Agencies will advise the Deputies or Principals of other consequences that may result from a change in watchlist status and seek guidance as to how to proceed.

1.59.6 After these categorical moves are accomplished or renewed, there will be an expedited procedure for the review of all U. S. PERSONS that are part of the TBU to ensure their watchlisting status is appropriate (including whether continued categorical watchlisting may be warranted based on the nature of the threat).

1.60 **Arbitration of Watchlisting Disputes.** If a NOMINATOR wishes to dispute TSC's watchlisting determination, it may contact NCTC (for international TERRORIST nominations) to discuss the watchlisting status and/or submit additional substantive derogatory and identifying information to support its initial nomination. Additional information provided to NCTC by a NOMINATOR will be passed to the TSC for review and final watchlisting determination. In the case of an FBI dispute over the TSC's watchlisting determination of an international TERRORIST'S nomination, a case agent must contact the TSC.

1.61 In the case of domestic TERRORIST nominations, if the FBI wishes to dispute TSC's watchlisting determination, it may contact the TSC to discuss the watchlisting status and/or submit additional substantive derogatory and identifying information to support its initial nomination.

## **X. PROCEDURES TO REMOVE AN INDIVIDUAL FROM THE WATCHLIST**

1.62 A NOMINATOR desiring to remove an international TERRORIST identity record previously nominated to TIDE should contact NCTC and provide written justification for the request. NCTC will promptly process the request when received. NCTC will be the final arbiter of whether the identity is removed from TIDE and TSC will be the final arbiter of whether TERRORIST IDENTIFIERS are removed from TSDB.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 1.63 If the NOMINATOR requesting removal of an international TERRORIST identity record from TIDE is the only NOMINATOR to have provided information on that record, the removal request will be immediately processed by NCTC. The removal information is then sent to the TSC, which, in turn, makes a determination regarding removal of the TERRORIST identity from the TSDB.
- 1.64 If multiple NOMINATORS have provided information on an international TERRORIST identity record, NCTC will coordinate with all relevant parties in an attempt to reach a consensus on the TERRORIST identity's most appropriate watchlisting status.
- 1.64.1 If the multiple NOMINATORS arrive at a consensus that the watchlisted identity is not reasonably suspected of engaging in TERRORISM and/or TERRORIST ACTIVITIES, or an applicable exception, the identity is removed from the TSDB and TIDE. In certain circumstances, NCTC may retain records in TIDE to prevent inappropriate re-watchlisting.
- 1.64.2 If the multiple NOMINATORS cannot arrive at a consensus regarding the watchlisting status of an identity, TSC may decide to remove the identity from the TSDB, but NCTC may retain the identity in TIDE.
- 1.64.3 For cases in which the FBI has conducted an investigation on an individual (independently nominated by another NOMINATOR) and has concluded that the watchlisted individual is not a KNOWN or SUSPECTED TERRORIST, the individual may be removed from the TSDB.<sup>34</sup> In such cases, the TERRORIST IDENTIFIERS from the FBI's investigation may be used to supplement the TIDE record.
- 1.65 The FBI will review domestic TERRORIST identity removal requests according to applicable FBI procedures.
- 1.66 TSC has an established, on-going process to review every record in the TSDB in accordance with Paragraph (8)(b) of the *TSC MOU* and its mission under HSPD-6 to maintain the most thorough, accurate, and current information in the TSDB. If TSC determines that the watchlisting standards are not met for an individual record, TSC will remove the record from the TSDB, in coordination with the NOMINATING AGENCY.

**XI. REDRESS PROCEDURES**

- 1.67 In January 2005, the TSC established a formal watchlist redress process that allows Agencies

---

<sup>34</sup> After an FBI determination that the individual is not a KNOWN or SUSPECTED TERRORIST, NCTC may determine based on a NOMINATOR's independent nomination- that the individual should remain in TIDE as records that have been fully vetted and should not be screened against (TIDE Category Code 140), the individual be watchlisted based upon the NOMINATOR's independent determination that the individual is a KNOWN or SUSPECTED TERRORIST or that the individual warrants watchlisting based upon an exception to the REASONABLE SUSPICION standard.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

that use TSDB data during a TERRORISM screening process to refer individuals' complaints to the TSC if it appears the complaints may be related to the watchlisting process. The goal of the watchlist redress process is to provide for timely and fair review of individuals' complaints and to identify and correct any errors in the TSDB.

- 1.68 The watchlist redress process is a multi-Agency process involving the DHS, TSC, NCTC, NOMINATORS, and SCREENERS. On September 19, 2007, Agencies participating in the watchlist redress process executed the *Redress MOU* to set forth a coordinated redress process to respond to individual complaints about adverse screening experiences.<sup>35</sup>
- 1.69 TSC's Redress Office is responsible for receiving, tracking, and researching watchlist-related complaints that SCREENERS refer to TSC. For each redress complaint received, the Redress Office conducts an in-depth analysis to determine if the person's complaint is related to a TSDB record, including a determination of whether the complainant is the watchlisted individual or merely a near-match to a watchlist record. If the complainant is the watchlisted individual, the TSC's Redress Office will determine whether the watchlisted individual still meets all the watchlisting criteria.
- 1.70 For each complaint, the TSC Redress Office coordinates with the NOMINATOR (via NCTC when the NOMINATOR is not the FBI), who assists in the evaluation of the complaint to ensure the most current, accurate, and thorough information available is used to review the person's watchlist status. Where appropriate and warranted by the current information and applicable criteria, a person's watchlist status may be adjusted (*e.g.*, downgraded from the No Fly to Selectee List or the person's identity may be removed entirely from the TSDB). If the redress complaint was referred to the TSC from the DHS Traveler Redress Inquiry Program (DHS TRIP), the individual's adjusted watchlist status will be provided to DHS TRIP for issuance of an appropriate response.
- 1.71 DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experience during their travel screening or inspection at, for example, transportation hubs like airports, or when crossing U.S. borders. The DHS TRIP website is [www.dhs.gov/trip](http://www.dhs.gov/trip). DHS TRIP ensures a thorough review is completed by consulting and sharing information with other DHS Components and other Agencies, as appropriate, to address the issues identified by the complainant.

**XII. PERIODIC REVIEW OF THE WATCHLISTING GUIDANCE**

- 1.72 This Watchlisting Guidance shall be reviewed no less than every two years following the conclusion of the previous review, or as needed.

---

<sup>35</sup> See Appendix 8, *Redress MOU*; see also FN 16, *supra*.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## CHAPTER 2: MINIMUM IDENTIFYING CRITERIA

### I. BIOMETRIC NOMINATIONS

- 2.1 Biometric information refers to the measurable biological (anatomical or physiological) and behavioral characteristics that can be used for recognition. Examples include facial photographs, fingerprints, iris scans, digital images, latent prints, DNA and gait. A biometric is sufficient to meet the minimum identifying criteria for nominations to the NCTC's TIDE and/or the TSC's TSDB, provided that the nomination also meets the minimum substantive derogatory criteria, or one of the exceptions. Biometric nominations without minimum biographic information will be provided only to those SCREENERS that have the technical capability to screen against or otherwise make assessments using the biometrics. Notwithstanding the above, all NOMINATORS are encouraged to include all available associated biographic information with any biometric nomination.

### II. MINIMUM BIOGRAPHIC NOMINATION REQUIREMENT

- 2.2 **TIDE.** NOMINATORS shall provide NCTC, for inclusion into TIDE, FRAGMENTARY INFORMATION that suggests an individual may have a nexus to TERRORISM and/or TERRORIST ACTIVITIES and any additional information that will facilitate identification of these individuals. Nominations to TIDE under this section will be considered for inclusion in the TSDB if the NOMINATING AGENCY believes there is REASONABLE SUSPICION to believe that the individual is a KNOWN or SUSPECTED TERRORIST.
- 2.2.1 Nominations of individuals based on FRAGMENTARY INFORMATION who fail to meet the minimum identifying criteria for nomination to TSDB should be provided to NCTC for inclusion in TIDE when there is DEROGATORY INFORMATION suggesting that the individual is associated with TERRORISM and the NOMINATING AGENCY determines that there are sufficient identifiers for possibly facilitating a match to existing TIDE records. Unless otherwise directed, NOMINATING AGENCIES should prioritize the nominations of individuals who satisfy the minimum identifying criteria before addressing nominations based on FRAGMENTARY INFORMATION.
- 2.3 **SCRENER Discretion.** As appropriate, SCREENERS have the discretion to decide not to include in their screening systems common names received from the TSDB, where insufficient identifying information exists for identification.
- 2.4 **TSDB.** Nominations to the TSDB must include a last name. NOMINATING AGENCIES should also provide any additional identifying information available. In addition to a last name, nominations must include:
- 2.4.1 first name;

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION****2.4.2 Or any one of the following additional identifiers:**

- 2.4.2.1 Full date of birth (eight digit "mm/dd/yyyy" format);
- 2.4.2.2 Passport number (with or without country of issuance);
- 2.4.2.3 Unique identifying numbers such as alien registration numbers, visa numbers, and social security numbers;
- 2.4.2.4 Telephone number(s)<sup>36</sup>;
- 2.4.2.5 E-mail address(es)<sup>37</sup>;
- 2.4.2.6 License plate number(s).

**2.4.3 Or any two of the following additional identifiers<sup>38</sup>:**

- 2.4.3.1 Country of citizenship, if different from place of birth;
- 2.4.3.2 Place of birth (city or country), if different from country of citizenship;
- 2.4.3.3 Circa or partial date of birth (partial: *e.g.*, 1960; or range: *e.g.*, 1960-1965);
- 2.4.3.4 Full name of an immediate family member (*e.g.*, parent, spouse, sibling, or children);
- 2.4.3.5 Occupation or current employer;
- 2.4.3.6 Specific degrees received;
- 2.4.3.7 Schools attended;
- 2.4.3.8 Physical identifiers such as race, height, or weight;
- 2.4.3.9 Unique physical identifiers such as scars, marks or tattoos;
- 2.4.3.10 Street address or other sufficiently specific location information.

<sup>36</sup> Only unclassified phone numbers that are authorized for passage to TSC pursuant to Paragraph 7(m) of Addendum B to the *TSC MOU*, will be included in TSDB. *See* Appendix 4. Unclassified phone numbers will only be provided to those SCREENERS that have the technical capability to receive this data.

<sup>37</sup> Only unclassified email addresses that are authorized for passage to TSC pursuant to Paragraph 7(m) of Addendum B of the *TSC MOU* will be included in TSDB. *See* Appendix 4. Unclassified email addresses will only be provided to those SCREENERS that have the technical capability to receive this data.

<sup>38</sup> As required here, there must be two distinct identifiers that must be sufficiently specific to account for the large number of possible matches common identifiers may produce. For example, if one identifier is rather common (*e.g.*, physical identifiers), the other identifier must be more specific to permit the screening official to successfully match a record with an individual. As a further example, a nomination with the last name listed as Khan, location listed as Kabul, Afghanistan, and occupation listed as a baker alone would be insufficient for screening purposes because it is highly unlikely a successful match could be made against such data. However, a nomination with the name listed as R. Khan, location listed as residence of 123 Sunshine Street, Kabul, Afghanistan, and occupation listed as a baker at ABC Bakery, would be sufficient for screening purposes.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**III. MINIMUM BIOGRAPHIC INFORMATION REQUIRED FOR EXCEPTIONS TO THE MINIMUM SUBSTANTIVE DEROGATORY STANDARDS FOR TERRORIST WATCHLISTING**

- 2.5 There are certain exceptions to the minimum substantive derogatory standards for TERRORIST watchlisting that support immigration and visa screening activities by DHS and DOS.<sup>39</sup> Examples of these categories of records include, but may not be limited to, records relating to an individual who has a defined relationship with the KNOWN or SUSPECTED TERRORIST, but whose involvement with the KNOWN or SUSPECTED TERRORIST'S activities is unknown (TIDE Category Code 50) and those with insufficient DEROGATORY INFORMATION TO meet the REASONABLE SUSPICION standard for watchlisting (TIDE Category Code 99).
- 2.6 NOMINATING AGENCIES should provide all additional identifying information available. All nominations under this section must include a **full name (first name, last name)** and one of the following identifiers:
- 2.6.1 Full date of birth;
  - 2.6.2 Full passport number (with or without country of issuance);
  - 2.6.3 Unique identifying numbers such as alien registration numbers, visa numbers, and social security account numbers;
  - 2.6.4 Telephone number(s);
  - 2.6.5 Email address(es);
  - 2.6.6 License plate number(s);
  - 2.6.7 Biometrics, such as facial image, iris scans or fingerprints.

---

<sup>39</sup> See Chapter 3, Section V.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**CHAPTER 3: MINIMUM SUBSTANTIVE DEROGATORY CRITERIA****I. INTRODUCTION AND PURPOSE**

- 3.1 TSC issued an updated U.S. Government Protocol Regarding Terrorist Nominations on February 25, 2009, that included an appendix identifying the minimum substantive derogatory criteria for acceptance of KNOWN or SUSPECTED TERRORIST nominations into the TSDB. Based on the attempted terror attack of December 25, 2009, the Watchlisting Guidance was reviewed to determine whether adjustments were needed. The revised guidance was approved by the White House Deputies Committee on May 25, 2010 and issued to the watchlisting community on July 16, 2010, after a multi-agency classification review.
- 3.2 This Chapter of the Watchlisting Guidance has been updated to reflect the watchlisting community's experiences with the Guidance since issuance in July of 2010 by the Deputies Committee. One of the more notable changes of this updated version of the Watchlisting Guidance is the restructuring of instances for when PARTICULARIZED DEROGATORY INFORMATION is required. Another notable change includes the re-introduction of guidance relative to the TERRORIST facilitators or supporters from an earlier version of the Watchlisting Guidance and the inclusion of additional exceptions to the minimum substantive derogatory standards for TERRORIST watchlisting that support immigration and visa screening activities of the DOS and DHS.

**II. REASONABLE SUSPICION**

- 3.3 For purposes of watchlisting an individual to the TSDB, the NOMINATOR should determine whether there is REASONABLE SUSPICION that an individual is a KNOWN or SUSPECTED TERRORIST.<sup>40</sup>
- 3.4 **REASONABLE SUSPICION.** To meet the REASONABLE SUSPICION standard, the NOMINATOR, based on the totality of the circumstances, must rely upon articulable intelligence or information which, taken together with rational inferences from those facts, reasonably warrants a determination that an individual is known or suspected to be or has been knowingly engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES. There must be an objective factual basis for the NOMINATOR to believe that the individual is a KNOWN or SUSPECTED TERRORIST. Mere guesses or hunches are not sufficient to constitute a REASONABLE SUSPICION that an individual is a KNOWN or SUSPECTED TERRORIST. Reporting of suspicious activity alone that does not meet the REASONABLE SUSPICION standard set forth herein is not a sufficient basis to watchlist an individual. The facts, however, given fair consideration, should sensibly lead to the conclusion that an individual is, or has, engaged in TERRORISM and/or TERRORIST ACTIVITIES.

---

<sup>40</sup> In instances where REASONABLE SUSPICION is not found, NOMINATORS should also determine whether the individual should be nominated to support immigration and visa screening by DHS and DOS (*see* Chapter 3, Section V).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 3.5 **Due Weight.** In determining whether a REASONABLE SUSPICION exists, due weight should be given to the specific reasonable inferences that a NOMINATOR is entitled to draw from the facts in light of his/her experience and not on unfounded suspicions or hunches. Although irrefutable evidence or concrete facts are not necessary, to be reasonable, suspicion should be as clear and as fully developed as circumstances permit. For additional guidance regarding the nomination of U.S. PERSONS, *see* Paragraph 3.15.
- 3.6 NOMINATORS shall not nominate an individual based on source reporting that NOMINATING personnel identify as, or know to be, unreliable or not credible. Single source information, including but not limited to "walk-in", "write-in", or postings on social media sites, however, should not automatically be discounted merely because of the manner in which it was received. Instead, the NOMINATING AGENCY should evaluate the credibility of the source, as well as the nature and specificity of the information, and nominate even if that source is uncorroborated, assuming the information supports a REASONABLE SUSPICION that the individual is a KNOWN or SUSPECTED TERRORIST or there is another basis for watchlisting the individual.
- 3.7 **Criteria and Data Quality.** To demonstrate that the nomination has sufficient indicia of reliability to support a REASONABLE SUSPICION determination, NOMINATING AGENCIES should incorporate processes designed to ensure that nominations are free of errors, and to the extent possible given the nature of the reporting, have not come from sources known or determined to be unreliable. NOMINATING AGENCIES should, to the extent possible, verify the accuracy and reliability of the information included in nominations. In addition to ensuring that nominations are free from errors, NOMINATING AGENCIES should implement procedures designed to ensure that recalled or revised information is reviewed regularly, and that necessary corrections to nominations based on those revisions/retractions are made.
- 3.8 **PARTICULARIZED DEROGATORY INFORMATION.** PARTICULARIZED DEROGATORY INFORMATION is the type of information relied on to determine whether REASONABLE SUSPICION is met. This is information that demonstrates the nature of an individual's or group's association with TERRORISM and/or TERRORIST ACTIVITIES that is descriptive and specific to an event or activity, and is more than a label. For example, "Subject X provides false travel documentation for Al-Qaida operatives" is PARTICULARIZED DEROGATORY INFORMATION, whereas "Subject Y is a supporter," standing alone, is not considered PARTICULARIZED DEROGATORY INFORMATION.
- 3.9 **Potential Behavioral Indicators.** In making a REASONABLE SUSPICION determination, NOMINATORS should consider behavioral indicators known to be associated with particular KNOWN or SUSPECTED TERRORISTS. The following is a list of a few examples of those indicators. It is not an exclusive list and it includes activity that may have innocent explanations wholly unrelated to TERRORISM. Furthermore, some activities conducted by U.S. PERSONS or activities taking place within the United States, may be an exercise of rights guaranteed by the First Amendment. Watchlisting an individual for engaging solely in

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

constitutionally protected activities is prohibited.<sup>41</sup> For these reasons, it is critical that each of these activities—as with all possible indicators of TERRORIST ACTIVITY—not be judged in isolation. Each must be viewed in the context in which it occurs and considered in combination with all other known information to ensure that any nomination based in whole or in part on this behavior comports with the standards set forth above:

- 3.9.1 Attendance at training camps known to the IC as facilitating TERRORIST ACTIVITIES<sup>42</sup>;
- 3.9.2 Attendance at schools/institutions identified by the IC as teaching an ideology that includes the justification of the unlawful use of violence or violent extremism;
- 3.9.3 Repeated contact with individuals identified by the IC as teaching or espousing an ideology that includes the justification of the unlawful use of violence or violent extremism; or,
- 3.9.4 Travel for no known lawful or legitimate purpose to a locus of TERRORIST ACTIVITY.

**III. KNOWN TERRORISTS****3.10 Definitions.**

3.10.1 **KNOWN TERRORIST.** A KNOWN TERRORIST is an individual whom the U.S. Government knows is engaged, has been engaged, or who intends to engage in TERRORISM and/or TERRORIST ACTIVITY, including an individual (a) who has been charged, arrested, indicted, or convicted for a crime related to TERRORISM by U.S. Government or foreign government authorities; or (b) identified as a TERRORIST or member of a designated foreign terrorist organization pursuant to statute, Executive Order or international legal obligation pursuant to a United Nations Security Council Resolution.

3.10.2 **TERRORISM and/or TERRORIST ACTIVITIES.** In general, TERRORISM and/or TERRORIST ACTIVITIES are acts that: (a) involve violent acts or acts dangerous to human life, property, or infrastructure that may be a violation of U.S. law, or may have been, if those acts were committed in the United States; and, (b) appear intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of government by mass destruction, assassination, kidnapping, or hostage-taking. This includes activities that facilitate or support

<sup>41</sup> See Chapter 1, Section III.

<sup>42</sup> Attendance at TERRORIST training camps alone meets the REASONABLE SUSPICION standard. Note that under the INA section 212 (a)(3)(B)(i)(VIII)[8 U.S.C. 1182(a)(3)(B)(i)(VIII)], an alien who has received military-type training (as defined in section 2339D(c)(1) of Title 18, United States Code) from or on behalf of any organization that, at the time the training was received, was a terrorist organization as defined in clause (vi), is inadmissible. Note also that 18 U.S.C. section 2339D criminalizes receiving military type training from a designated foreign terrorist organization.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

TERRORISM and/or TERRORIST ACTIVITIES.<sup>43</sup>**3.11 Types of KNOWN TERRORISTS for Whom REASONABLE SUSPICION is Established by Recognized Authority and for Whom Particularized Derogatory Information is Not Required.**

**3.11.1 Arrested or Convicted TERRORISTS.**<sup>44</sup> Individuals who have been arrested or convicted for TERRORIST ACTIVITY are considered KNOWN TERRORISTS who should be nominated. The arrest or conviction is presumed to meet the REASONABLE SUSPICION standard for watchlisting unless there is reason to believe that the information is questionable (e.g., faulty or erroneous), of dubious origin (e.g., poison pen, source known to be unreliable, or politically motivated) or the result of an unreliable process (e.g., conviction by a court that does not adhere to minimally acceptable due process standards). Nominations should include the charge, location, and date of the arrest or conviction, if available.

**3.11.2 Individuals Identified Pursuant to Statute or Executive Order.**<sup>45</sup> Pursuant to Executive Order 13224, as amended, "Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism," Executive Order 12947, as amended, "Prohibiting Transactions with Terrorists Who Threaten to Disrupt the Middle East Peace Process," and section 302 of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) publishes, updates, and maintains an integrated and comprehensive list of designated parties with whom U.S. PERSONS are prohibited from providing services or conducting transactions and whose assets are blocked. The names on this list include persons designated under country-based and list-based economic sanctions programs, as well as individuals and entities designated under the various Executive Orders and Statutes aimed at TERRORISM. Persons designated under Executive Order 13224, Executive Order 12947, or the AEDPA are included on this integrated and comprehensive list and are 'Specially Designated Global Terrorists' (SDGTs), 'Specially Designated Terrorists' (SDTs), or 'Foreign Terrorist

<sup>43</sup> TERRORISM and/or TERRORIST ACTIVITIES include acts that the actor knows or reasonably should know affords material support to any individual who the actor knows or reasonably should know, has committed or plans to commit a terrorist activity, to a terrorist organization or to any member of such an organization. Material support includes providing a safe house, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training for the commission of an act of TERRORISM and/or TERRORIST ACTIVITY.

<sup>44</sup> See Paragraph 3.13.1 for situations involving individuals who are acquitted or against whom charges are dismissed for a crime related to TERRORISM.

<sup>45</sup> These authorities generally authorize the Secretary of State (in consultation with either the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, or a combination thereof) to designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of TERRORISM that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States. Additionally, leaders or members of a Foreign Terrorist Organization (FTO), an Specially Designated Global Terrorist (SDGT) under Executive Order 13224, or an organization named to the Terrorist Exclusion List (TEL) may be designated as a terrorist organization by the Secretary of State for immigration purposes pursuant to INA section 212(a)(3)(B)(vi)(II) [8 U.S.C. 1189(a)(3)(B)(vi)(II)].

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

Organizations' (FTOs), respectively, and should be nominated accordingly.<sup>46</sup> NOMINATORS should regularly check the Specially Designated Nationals List (SDNL) as individuals are added and dropped as new information becomes available.

**3.11.3 Individuals Identified as TERRORISTS Pursuant to a United Nations Security Council Resolutions (UNSCR) Concerning Al-Qaida and Associated Individuals and Entities.** Under UNSCR resolution 1267 (1999), modified and strengthened by subsequent resolutions, including resolutions 1333 (2000), 1390 (2002), 1445 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), and resolution 1989 (2011), sanctions measures now apply to designated individuals and entities associated with Al-Qaida, wherever located. The names of the targeted individuals and entities are placed on the Al-Qaida Sanctions List.<sup>47</sup> Under the UNSCR sanctions regime, the United States has an international legal obligation to prevent the entry into or transit through its territory of designated individuals listed on the Al-Qaida Sanctions List.<sup>48</sup> NOMINATORS should regularly check the Al-Qaida Sanctions List as individuals are added and dropped as new information becomes available.

**3.11.4 Individuals Identified as TERRORISTS Pursuant to the National Intelligence Priorities Framework of Counterterrorism.** Members of groups (not support entities) that are identified on the National Intelligence Priorities Framework of Counterterrorism, (NIPF-CT) are presumed to meet the REASONABLE SUSPICION standard so long as the group name is not just a regional or activity-based characterization. Neutral associations such as janitorial, repair, or delivery services of commercial goods do not meet the REASONABLE SUSPICION standard.

**IV. SUSPECTED TERRORISTS****3.12 Definition.**

**3.12.1** A SUSPECTED TERRORIST is an individual who is REASONABLY SUSPECTED to be, or has been, engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES based on an articulable and REASONABLE SUSPICION.

**3.13 Types of SUSPECTED TERRORISTS.**

<sup>46</sup> The comprehensive list of SDGTs and SDTs is accessible through the OFAC website at the following URL: <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>

<sup>47</sup> Narrative summaries of the reasons for listing individuals, groups, undertakings and entities on the Al-Qaida Sanctions List (where available) can be found at the following URL: <http://www.un.org/sc/committees/1267/narrative.shtml>.

<sup>48</sup> Many persons designated under UNSCR 1267 and Executive Order 13224 are or have been engaged in financial support, facilitation, and other activities in support of TERRORISM. They often, however, do not meet the current criteria for placement on the No Fly List. DHS and DOS will review the information provided about these individuals and take actions, as appropriate.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 3.13.1 **Individuals Who are Acquitted or for Whom Charges are Dismissed.** An individual who is acquitted or against whom charges are dismissed for a crime related to TERRORISM may nevertheless meet the REASONABLE SUSPICION standard and appropriately remain on, or be nominated to, the Terrorist Watchlist.<sup>49</sup> Each case should be evaluated based on the facts of the underlying activities, the circumstances surrounding the acquittal or dismissal, and all known DEROGATORY INFORMATION to determine if the individual should remain on the Terrorist Watchlist.
- 3.13.2 **Individuals Identified as TERRORISTS Pursuant to Other Internal Department or Agency Processes.** Departments or Agencies that nominate individuals associated with a terrorist group that is not designated by Statute or Executive Order (*see* Paragraph 3.11.2) or groups that fall outside of the NIPF-CT construct (*see* Paragraph 3.11.4) must have internal processes to review the activities of TERRORISTS and terrorist organizations. So long as a Department's or Agency's internal process has determined that a group is engaging in TERRORISM and/or TERRORIST ACTIVITIES, REASONABLE SUSPICION can be met for members of the group, or active participants in, that group's TERRORIST ACTIVITIES. Departments and Agencies that use this clause to recommend subjects for watchlisting are required to provide written notice to NCTC and TSC (an email will suffice) of the Department or Agency's determination. While members or active participants of such groups may be nominated without PARTICULARIZED DEROGATORY INFORMATION, the watchlisting of an individual pursuant to this clause must be based on the determination by a Department or Agency's internal processes that the group is engaging in TERRORISM and/or TERRORIST ACTIVITIES. Neutral associations like janitorial, repair, or delivery services of commercial goods do not meet the REASONABLE SUSPICION standard.
- 3.13.3 **Individuals Identified as TERRORISTS Pursuant to Agreements by U.S. Government Agencies/Foreign Governments for Sharing of TERRORIST Identity Data.** The U.S. Government may enter into agreements with foreign governments for the sharing of TERRORIST identity information. Pursuant to such agreements, data will be provided to the TSC for TERRORIST screening, as required under HSPD-6. The Information Sharing and Access (ISA) Interagency Policy Committee (IPC) or an IPC-designated interagency body, will make a determination, country by country, prior to the final agreement on whether the data provided will (1) be presumed to meet the standard for inclusion in TSDB; or (2) undergo the Foreign Partner Vetting Process.
- 3.13.4 **Individuals Identified as Associates or Affiliates of KNOWN or SUSPECTED TERRORISTS or TERRORIST Cells or Networks.**<sup>50</sup> Individuals who are associated or affiliated with a KNOWN or SUSPECTED TERRORIST, or TERRORIST cells or networks should be nominated when there is PARTICULARIZED DEROGATORY INFORMATION

<sup>49</sup> Because the REASONABLE SUSPICION standard required for watchlisting is lower than that required for a criminal conviction (*i.e.*, beyond a reasonable doubt), an individual that is acquitted or for whom charges are dismissed may qualify for watchlisting based on the facts and circumstances surrounding the acquittal or dismissal.

<sup>50</sup> This section applies as well to persons "linked to," "related" and other similar descriptors to a KNOWN or SUSPECTED TERRORIST, TERRORIST cells or networks.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

regarding the context of the relationship that gives rise to a REASONABLE SUSPICION that the individual is engaging or has engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES. Neutral associations such as janitorial, repair, or delivery services of commercial goods are not sufficient. Information about the pertinent activities of the KNOWN or SUSPECTED TERRORIST, TERRORIST cell or network should be included in the nomination. These nominations should include context or content to demonstrate the membership, association, or affiliation to the KNOWN or SUSPECTED TERRORIST, TERRORIST cell or network. Individuals who merely "may be" members, associates or affiliates to a terrorist organization may not be accepted into the TSDB, unless the REASONABLE SUSPICION standard is met and PARTICULARIZED DEROGATORY INFORMATION accompanies the nomination.

**3.13.4.1 Inferences that Support REASONABLE SUSPICION.** REASONABLE SUSPICION may be rationally inferred from the context of the relationship with the KNOWN or SUSPECTED TERRORIST. The following factors should be considered when determining whether REASONABLE SUSPICION may be inferred:

**3.13.4.1.1** The nature of the activity engaged in with the KNOWN or SUSPECTED TERRORIST;

**3.13.4.1.2** The frequency, duration, or manner of their contact;

**3.13.4.1.3** A close, continuing, or direct relationship with a KNOWN or SUSPECTED TERRORIST that reasonably suggests the individual is knowingly involved in or willfully supporting the KNOWN or SUSPECTED TERRORIST'S TERRORIST ACTIVITIES; or,

**3.13.4.1.4** Other malevolent or illicit factors that can be articulated that would support a REASONABLE SUSPICION that the individual is engaging in TERRORISM and/or TERRORIST ACTIVITIES.

**3.13.5 Individuals Identified as TERRORIST Facilitators.** TERRORIST facilitators are presumed to meet the REASONABLE SUSPICION standard. The nomination should include PARTICULARIZED DEROGATORY INFORMATION concerning the type of "facilitation" involved and the role of the facilitator when this information is known. Individuals who are considered facilitators include, but are not limited to, financial fundraisers, document forgers, travel facilitators, money launderers, and arms merchants. There must be REASONABLE SUSPICION that the facilitator knew that his or her actions would aid in the furtherance of TERRORISM and/or TERRORIST ACTIVITIES.

**3.13.5.1 Criminal Activity Supporting TERRORISM.** If intelligence or information indicates that the individual is engaging in criminal activity related to smuggling, providing safe houses, forging documents, or any other support to TERRORISTS or terrorist groups, NOMINATORS should presume that the individual is knowingly engaging in criminal activity that supports TERRORISM and/ or TERRORIST

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

ACTIVITIES. In these circumstances, REASONABLE SUSPICION is based on the TERRORIST criminal activity and should be described in the nomination.

**3.13.6 Individuals who Incite Others to Commit Acts of TERRORISM.**<sup>51</sup> Inciting an individual to commit an act of TERRORISM and/or TERRORIST ACTIVITIES under circumstances that indicate an intention to cause death or serious bodily harm is considered engaging in TERRORIST ACTIVITY and is sufficient to meet the REASONABLE SUSPICION standard. The nomination should include PARTICULARIZED DEROGATORY INFORMATION concerning the type of "incitement" involved and the role of the individual when this information is known. Normally, speech will not rise to the level of "inciting" unless there is a clear link between the speech and an actual effort to undertake the TERRORIST ACTIVITY. The individual may have incited TERRORIST ACTIVITY, even if a terrorist attack does not actually occur (*e.g.*, because an attempt to commit such activity is thwarted). Speech advocating a violent or dangerous TERRORIST ACTIVITY is incitement if such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.<sup>52</sup>

**3.13.7 Individuals Who Solicit Others to Engage in TERRORIST ACTIVITIES.** In an individual capacity or as a member of an organization, any individual who solicits another to engage in a TERRORIST ACTIVITY and/or for membership in a terrorist organization is considered to be engaging in TERRORIST ACTIVITY. Nominations that include PARTICULARIZED DEROGATORY INFORMATION concerning the type of solicitation involved and the role of the individual are sufficient to meet the REASONABLE SUSPICION standard. An individual may fall outside the scope of engaging in the solicitation of an individual for membership in a terrorist organization if there is information that demonstrates that the individual did not know and should not have reasonably known that the organization was a terrorist organization.

**3.13.8 Individuals Identified as Sympathizers and Supporters of a Designated Terrorist Organization.**<sup>53</sup> Sympathizers and supporters of a designated terrorist organization (DTO) (*see* Paragraph 3.11.2) may be watchlisted when the REASONABLE SUSPICION standard is met, and the nomination includes PARTICULARIZED DEROGATORY INFORMATION concerning the how the individual's activities warrant watchlisting, as opposed to information about why the organization is a DTO.

**3.13.8.1** A sympathizer or supporter of TERRORISM should be nominated if the support is operational in nature. If support is merely ideological, the individual should not be nominated.

<sup>51</sup> For situations where there is no PARTICULARIZED DEROGATORY INFORMATION, individuals may be watchlisted as an exception to the REASONABLE SUSPICION standard. *See* Paragraph 3.14.3.

<sup>52</sup> *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 122 S.Ct. 1389 (2002); 9 FAM 40.32 N2.5, "Advocacy of Terrorism Not Always Exclusionary."

<sup>53</sup> For situations where there is no PARTICULARIZED DEROGATORY INFORMATION, supporters of a designated terrorist organization (DTO) may be watchlisted as an exception to the REASONABLE SUSPICION standard. *See* Paragraph 3.14.4.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**3.13.9 Individuals Identified as FOREIGN FIGHTERS.** FOREIGN FIGHTERS are defined as nationals of one country who travel or attempt to travel to another country to participate in TERRORISM and/or TERRORIST ACTIVITIES, and to the extent possible, the nomination should include PARTICULARIZED DEROGATORY INFORMATION. Behavior that qualifies as PARTICULARIZED DEROGATORY INFORMATION is the travel to a foreign country to participate in TERRORISM and/or TERRORIST ACTIVITIES.

**3.13.9.1** A person is not considered a FOREIGN FIGHTER when he or she traveled from Country A to Country B for non-TERRORIST reasons (*e.g.*, enrolling in school). Inferences that someone is a FOREIGN FIGHTER may not be drawn solely from biographic facts that indicate a person was born in one country and is found in a different country and suspected to be participating in TERRORISM and/or TERRORIST ACTIVITIES.

**3.13.10 Special Consideration for Individuals Involved with TERRORIST-Associated Weapons.** Individuals who possess, handle, use, manufacture, sell, or transfer Improvised Explosive Devices (IEDs), Explosively Formed Penetrators (EFP), Radiological Dispersion Devices (RDD), or improvised chemical, biological, radiological, or nuclear (CBRN) devices, are presumed to meet the REASONABLE SUSPICION standard due to the inherently dangerous nature of these items or when it can reasonably be inferred from the context that there is a connection to TERRORISM and/or TERRORIST ACTIVITIES (*e.g.*, Iraq, presence of other KNOWN or SUSPECTED TERRORISTS, previous attacks on or threats to U.S. Forces).

**3.13.11 Targets of Raids Conducted by the U.S. Military or the Intelligence Community.** REASONABLE SUSPICION is presumed where an individual was identified as the target of a raid to disrupt a FTO. When an individual is identified by discovery of information found during the course of such a raid conducted by the U.S. Military or the IC, however, REASONABLE SUSPICION is met where the available PARTICULARIZED DEROGATORY INFORMATION explains why he or she can be reasonably suspected of engaging or having engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITY. If there is no PARTICULARIZED DEROGATORY INFORMATION on the individual for whom information was discovered during the raid, he or she should not be nominated.

**3.13.12 Individuals Identified as TERRORISTS via Documentation or Media Exploitation Efforts.** Any individuals identified in documents or media otherwise captured by U.S. or allied forces or obtained from a NOMINATING AGENCY must have a connection to TERRORISM and/or TERRORIST ACTIVITIES in order to be nominated to the Terrorist Watchlist. REASONABLE SUSPICION for an individual to be nominated from document and media exploitation (DOMEX) materials may be established either by the content or context of the DOMEX, or other sources. Nominations under this section must include PARTICULARIZED DEROGATORY INFORMATION. For example, REASONABLE SUSPICION for watchlisting can be met based on the acquisition of documents/media identifying a person from the counterterrorism operation that targeted the residence of Al-Qaida

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

leader Usama bin Laden on May 2, 2011.<sup>54</sup> Likewise, individuals listed on a roster of an IED cell could be nominated solely on the presence of their name on the list. An identity from a captured passport, however, would only be watchlisted if additional reporting documents REASONABLE SUSPICION to believe that the individual is connected to TERRORISM and/or TERRORIST ACTIVITY.

- 3.13.13 **LONE WOLVES.** Because the focus is on the individual's TERRORISM-related conduct, "LONE WOLF" TERRORISTS should be nominated when PARTICULARIZED DEROGATORY INFORMATION and their actions support a REASONABLE SUSPICION that they are engaged in, or have engaged in, TERRORISM and/or TERRORIST ACTIVITIES. No present known affiliation with a terror group, organization, or cell is required but prior affiliations, if they exist, may be taken into account for supporting a rational inference that the individual is reasonably suspected of engaging in TERRORISM and/or TERRORIST ACTIVITIES.

## **V. EXCEPTIONS TO SUPPORT IMMIGRATION AND VISA SCREENING ACTIVITIES BY DHS AND DOS**

- 3.14 **TSDB Minimum Substantive Derogatory Exceptions to Support Immigration and Visa Screening Activities by the DHS and DOS.** The Watchlisting Guidance contains certain exceptions to the minimum substantive derogatory criteria for TERRORIST watchlisting that support immigration and visa screening activities by the DHS and DOS to determine whether grounds exist to deny admission of aliens to the United States (including denials of visas) or to deny other immigration benefits pursuant to the INA.<sup>55</sup> PARTICULARIZED DEROGATORY INFORMATION is not required for nominations made pursuant to the following sections. Because the INA defines "aliens" as "any person not a citizen or national of the United States"<sup>56</sup>, the INA admissibility provisions also apply to LPRs, in certain circumstances including those described in INA section 101(a)(13)(C)[8 U.S.C. 1101(a)(13)(C)], who are considered as U.S. PERSONS under Executive Order 12333. Consequently, NCTC developed a mechanism in TIDE to identify and distinguish U.S. citizens from non-U.S. citizens in order to further distinguish between "aliens" under the INA and U.S. PERSONS under Executive Order 12333. The following subsections are exceptions to the REASONABLE SUSPICION standard and will only be transmitted to DOS's CLASS (via the DOS CCD) and DHS's WLS to support immigration and visa screening processes.

<sup>54</sup> Such documents/media, however, still need to be reviewed to ensure that innocent individuals are not erroneously watchlisted.

<sup>55</sup> INA section 212(a)(3)(B)[8 U.S.C. 1182(a)(3)(B)] sets forth several grounds for inadmissibility based on terrorist activities, which is defined in INA section 212(a)(3)(B)(ii)[8 U.S.C. 1182(a)(3)(B)(iii)]. For example, INA section 212(a)(3)(B)(i)(VII) states that any alien who "endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization" is inadmissible to the United States. 8 U.S.C. 1182(a)(3)(B)(i)(VII). All other uses of the term "terrorist activities" within this Watchlisting Guidance that do not specifically reference the INA follow the definition outlined in Chapter I and Appendix 1.

<sup>56</sup> See INA § 101(a)(3)[8 U.S.C. 1101(a)(3)].

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

3.14.1 **Spouses and Children.** Spouses and children<sup>57</sup> of a KNOWN or SUSPECTED alien TERRORIST cannot be considered TERRORISTS without a REASONABLE SUSPICION that they are engaging or have engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES.<sup>58</sup> The INA provides that the alien spouse or alien child of an alien who is inadmissible for certain specified reasons relating to terrorist activities, if the activity causing the alien to be found inadmissible occurred within the last five (5) years, is inadmissible.<sup>59</sup> An alien spouse or child of an alien who is believed to be inadmissible under the INA for terrorist activities should be nominated. No additional DEROGATORY INFORMATION (in addition to familial relation) is required for nomination under this section, if the individual meets the below qualifications.

3.14.1.1 To qualify for watchlisting, alien spouses and children of a KNOWN or SUSPECTED TERRORIST must:

3.14.1.1.1 Be an alien (not a U.S. citizen or national), which includes LPRs; and,

3.14.1.1.2 Be an unmarried child under the age of 21 or a spouse of an alien.

3.14.1.2 Ex-spouses, widows, or widowers should not be nominated unless there is a REASONABLE SUSPICION to believe that they themselves are engaging or have engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES. Deceased spouses should not be nominated unless they are specifically covered in Paragraph 3.17.

3.14.1.3 Once a spouse or child no longer meets the definitional requirements under this section, such an individual should no longer be watchlisted unless there is a REASONABLE SUSPICION to believe that the individual is engaging in TERRORISM and/or TERRORIST ACTIVITIES. For example, if a child reaches the age of 21 and there is REASONABLE SUSPICION to believe he or she was knowingly involved in TERRORIST ACTIVITY by providing material support to a FTO, he or she can remain watchlisted based upon this DEROGATORY INFORMATION. On the other hand, once a child of a KNOWN or SUSPECTED TERRORIST turns 21 years of age, the individual should no longer be watchlisted under this exception because he or she is not considered a child of the KNOWN or SUSPECTED TERRORIST and additional DEROGATORY INFORMATION would be needed to meet the REASONABLE SUSPICION standard.

<sup>57</sup> The INA defines "child" as "an unmarried person under 21 years of age. . . ." INA § 101(b)(1)[8 U.S.C. 1101(b)(1)].

<sup>58</sup> The discussion in Paragraph 3.14.1 is limited exclusively to spouses and children; all other family members (including mothers, fathers, sisters and brothers) should be nominated for inclusion in the TSDB only if there is DEROGATORY INFORMATION that the individual has a close connection to a KNOWN or SUSPECTED TERRORIST and that connection meets the REASONABLE SUSPICION standard. Absent independent DEROGATORY INFORMATION, records for these individuals may be retained in TIDE for analytic purposes. See Paragraph 1.53.2.2 for treatment of these other family members as "non-TERRORIST" records that may reside in TIDE for analytic purposes but are not exported to the TSDB (known as TIDE Category Code 160).

<sup>59</sup> See INA § 212(a)(3)(B)(i)(IX)[8 U.S.C. 1182(a)(3)(B)(i)(IX)]. While this provision does not apply when the activity causing the alien to be found inadmissible occurred more than 5 years before the spouse or child's admissibility is being considered, the analysis of the time limit's application will be determined by SCREENERS upon ENCOUNTER.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 3.14.2 **Endorsers and Espousers.** An alien who endorses or espouses TERRORIST ACTIVITY or persuades others to endorse or espouse TERRORIST ACTIVITY or support a terrorist organization may be inadmissible under the INA and should be nominated.
- 3.14.3 **Incitement.** Inciting an individual to commit an act of TERRORISM and/or TERRORIST ACTIVITY under circumstances that indicate an intention to cause death or serious bodily harm is considered engaging in TERRORIST ACTIVITY. The individual may be inadmissible under the INA and should be nominated.
- 3.14.4 **Supporters of a Designated Terrorist Organization.** Supporters of a DTO may be inadmissible under the INA and should be nominated if the support is operational in nature. If support is merely ideological, the individual should not be nominated.
- 3.14.5 **Representatives.** Representatives of terrorist organizations and representatives of any political, social or other group that endorses or espouses TERRORIST ACTIVITY may be inadmissible under the INA and should be nominated. Representatives include an officer, official, or spokesman of an organization, and any person who directs, counsels, commands, or induces an organization to engage in TERRORIST ACTIVITY. Neither membership in, nor association with, the organization or group is required.
- 3.14.6 **TERRORISTS, Extremists, Jihadists, Militants, Mujahideen or Insurgents.**<sup>60</sup> Nominations of individuals described by sources as "TERRORISTS", "extremists", "jihadists", "militants", "mujahideen" or "insurgents"<sup>61</sup>, (an exclusive list) will be accepted into the TSDB as exceptions for export to DHS' WLS and DOS' CLASS-VISA and CLASS-PASSPORT for immigration and border processing when the following four conditions apply:
- 3.14.6.1 The individual is not a U.S. Citizen or National (e.g., the individual is a foreign national or a LPR);
  - 3.14.6.2 The context suggests a nexus to TERRORISM;
  - 3.14.6.3 Adequate identifiers are available to permit identification<sup>62</sup>; and,
  - 3.14.6.4 The information has been evaluated as being credible.
  - 3.14.6.5 It is important to recognize that some activities associated with extreme political or religious views expressed by aliens in the United States may constitute the exercise of rights guaranteed by the First Amendment (e.g., the rights to free speech, assembly and religious exercise).<sup>63</sup> Therefore, someone so labeled based

<sup>60</sup> This exception is commonly referred to as "label plus" nomination.

<sup>61</sup> Insurgency is defined as an "organized movement" aimed at the overthrow of a constituted government through the use of subversion and armed conflict.

<sup>62</sup> An adequate identifier is a biometric, or a last name, first name and any one of the additional identifiers listed in Chapter 2, Section II.

<sup>63</sup> See Chapter I, Section III concerning constitutionally protected activities.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

in part on this type of constitutionally protected activity, must have other substantive DEROGATORY INFORMATION indicative of TERRORIST intent. As previously noted, nominations may not be made based solely on protected activity.

- 3.14.7 **Additional Derogatory Information Required (TIDE Category Code 99s and 50s).** NCTC will retain a record in TIDE if it is determined that the information pertains to, or is related to, TERRORISM.<sup>64</sup> However, if a record involving an alien, which includes LPRs, does not contain sufficient DEROGATORY INFORMATION to meet any of the aforementioned exceptions to the TSDB's REASONABLE SUSPICION standard for inclusion, NCTC will generally designate the record as a Category Code 99 (the TIDE category code "applied when DEROGATORY INFORMATION does not meet the REASONABLE SUSPICION standard for watchlisting because it is very limited or of suspected reliability but there is a possible nexus to TERRORISM") or a Category Code 50 (the TIDE category code applied when an individual has a defined relationship with the KNOWN or SUSPECTED TERRORIST, but whose involvement with the KNOWN or SUSPECTED TERRORIST's activities is unknown)<sup>65</sup>, making it available for export to TSDB for use by DOS and DHS for visa adjudication and immigration processing.

## VI. SPECIAL CONSIDERATIONS

- 3.15 **Nominations of U.S. PERSONS.** Nominations of U.S. PERSONS, in accordance with the Attorney General approved procedures applicable to each element of the IC<sup>66</sup>, will be made pursuant to the procedures set forth below to ensure compliance with this REASONABLE SUSPICION standard. Nominations of U.S. PERSONS shall be made based on information from sources of known reliability or where there exists additional corroboration or context supporting REASONABLE SUSPICION. NOMINATING AGENCIES will review information on U.S. PERSONS pursuant to procedures set forth below consistent with the nature of the reporting supporting the nomination and the protection of sources and methods.

- 3.15.1 Special handling is warranted for U.S. PERSONS nominated for watchlisting, especially by an Agency other than the FBI. To ensure compliance with the Watchlisting Guidance that the REASONABLE SUSPICION standard exists for U.S. PERSONS in the TSDB, as well as to ensure proper interagency coordination, a formal process has been implemented that:

- 3.15.1.1 Ensures the FBI is aware of U.S. PERSONS nominated by any other Department or Agency;

---

<sup>64</sup> See Paragraph 1.26.

<sup>65</sup> See FN 28, *supra*.

<sup>66</sup> The referenced procedures are those approved for each element of the IC pursuant to Executive Order 12333, as amended, which states in relevant part, "Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a Department containing such element and approved by the Attorney General, consistent with the authorities provided by part 1 of this Order after consultation with the Director." See Executive Order 12333, Paragraph 2.3, as amended by Executive Order 13618 (July 6, 2012).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 3.15.1.2 Requires review of the watchlist nomination decision and concurrence by the TSC that REASONABLE SUSPICION exists for watchlisting;
  - 3.15.1.3 Ensures there is interagency awareness of all U.S. PERSON nominations (FBI or otherwise); and,
  - 3.15.1.4 Ensures there is U.S. Government coordination in the investigation and/or intelligence gathering on these individuals, including strategies for engagement with foreign partners if required.
- 3.15.2 NCTC should include in TIDE U.S. PERSONS who are under International TERRORISM Preliminary Investigation by the FBI but who have not been deemed to meet the REASONABLE SUSPICION standard and U.S. PERSONS with a nexus to TERRORISM, but for whom there is insufficient DEROGATORY INFORMATION to support entry in TSDB. These TIDE records on U.S. PERSONS will not be provided to TSC for export via the TSDB unless approved of as an exception to the REASONABLE SUSPICION standard pursuant to Section V in this Chapter of the Watchlisting Guidance, *infra*, or as part of a TBU pursuant to Paragraph 1.59 of the Watchlisting Guidance.
- 3.15.3 For U.S. PERSONS nominated by other Government Agencies who are not under FBI investigation, NCTC analysts receive, process, and export these subjects for inclusion in the TSDB, as appropriate under current procedures. As part of the processing, NCTC analysts identify and share these U.S. PERSON identifiers with the FBI's Foreign Terrorist Tracking Task Force (FTTTF) for assessment, and notifying the FBI case agent of the inclusion.
- 3.16 **Political Figures or Purposes.** Heads of State or other Government officials should be nominated when there is PARTICULARIZED DEROGATORY INFORMATION to support a REASONABLE SUSPICION to believe the individual is engaging or has engaged in conduct constituting, in preparation for, in aid of, or related to TERRORISM and/or TERRORIST ACTIVITIES. Waivers or other appropriate action can be requested from U.S. Customs and Border Protection (CBP) in coordination with DOS to facilitate the travel of a properly watchlisted Head of State or other government officials to the extent necessary.
- 3.16.1 Watchlisting an individual is prohibited based on political purposes, retaliation, or any other reason unconnected to the REASONABLE SUSPICION standard.
- 3.17 **Identities of Deceased Individuals.**
- 3.17.1 The TSDB will not include identity information of KNOWN or SUSPECTED TERRORISTS that are confirmed dead<sup>67</sup> unless:

---

<sup>67</sup> Subjects are considered "confirmed dead" under the following circumstances:

- a. The subject's death became a high profile case in the public sphere (*e.g.*, media footage confirming suicide bombers' deaths, 9/11 hijackers, death of Abu Musaq al Zarqawi); or,
- b. Reporting on the subject's death has been corroborated by at least two credible sources (*e.g.*, United States or "friendly" foreign government, fully-vetted asset).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 3.17.1.1 PARTICULARIZED DEROGATORY INFORMATION supports a REASONABLE SUSPICION that an existing KNOWN or SUSPECTED TERRORIST is using that identity information; or,
- 3.17.1.2 A recognized terrorist organization<sup>68</sup> collects KNOWN or SUSPECTED TERRORIST identity information for use by its members in preparing for or committing TERRORIST acts and identity or travel documents (e.g., related to a deceased KNOWN or SUSPECTED TERRORIST of that organization) have not been recovered. "Trusted travel documents" include all documents used for border crossings.
- 3.17.2 NOMINATING AGENCIES will share information regarding a watchlisted or nominated individual's deceased status under Addendum B of the *TSC MOU*, section (7)(m) ("Any other TERRORISM INFORMATION that ORIGINATORS specifically provide for passage to the TSC"). NCTC will export deceased status to the TSC, and the TSC will export deceased status to end user screening systems. NOMINATING AGENCIES will mark deceased status information "TIDE Restricted" in cases where the status, because of sensitive sourcing, should not be forwarded to the TSC. TIDE restricted information will not be exported to the TSC. When a nomination is made on a deceased person in accordance with this paragraph, the status indicator within TIDE that is exported to the TSC will be marked to reflect that the person is deceased.

**VII. EXAMPLES OF TERRORISM AND/OR TERRORIST ACTIVITIES**

- 3.18 Examples of TERRORISM and/or TERRORIST ACTIVITIES may generally include conduct intended to intimidate, coerce, influence, or affect civilian populations or government policy consisting of:
  - 3.18.1 destruction of aircraft or aircraft facilities (18 U.S.C. 32);
  - 3.18.2 violence at international airports (18 U.S.C. 37);
  - 3.18.3 biological weapons (18 U.S.C. 175 or 175b);
  - 3.18.4 variola virus (18 U.S.C. 175c);
  - 3.18.5 chemical weapons (18 U.S.C. 229);
  - 3.18.6 assassination and kidnapping of Congressional Members, Cabinet Officials, and Supreme Court Justices (18 U.S.C. 351 (a)(b)(c) or (d));
  - 3.18.7 nuclear materials (18 U.S.C. 831);
  - 3.18.8 participation in nuclear and weapons of mass destruction threats to the United States (18 U.S.C. 832);
  - 3.18.9 plastic explosives (18 U.S.C. 842(m) or (n) footnote 1.);
  - 3.18.10 arson and bombing of Government property risking or causing death (18 U.S.C. 844(f)(2) or (3));
  - 3.18.11 arson and bombing of property used in interstate commerce (18 U.S.C. 844(i));

---

<sup>68</sup> A classified list of recognized terrorist organizations that are known to reuse TERRORIST identity information is available on the Watchlisting Community of Interest portal on NCTC Current.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 3.18.12 killing or attempted killing during an attack on a Federal facility with a dangerous weapon (18 U.S.C. 930(c));
- 3.18.13 conspiracy to murder, kidnap, or maim persons abroad (18 U.S.C. 956(a)(1));
- 3.18.14 damaging a protected computer used in interstate or foreign commerce or that is used exclusively by a financial institution or the United States Government (18 U.S.C. 1030(a)(1); 18 U.S.C. 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v));
- 3.18.15 killing or attempted killing of officers and employees of the United States (18 U.S.C. 1114);
- 3.18.16 murder or manslaughter of foreign officials, official guests, or internationally protected persons (18 U.S.C. 1116);
- 3.18.17 hostage taking (18 U.S.C. 1203);
- 3.18.18 damage to Government property (18 U.S.C. 1361);
- 3.18.19 destruction of communication lines, stations, or systems (18 U.S.C. 1362);
- 3.18.20 injury to U.S. aircraft or vessels (18 U.S.C. 1363);
- 3.18.21 injury to U.S. diplomatic, consular, military, or other property (18 U.S.C. 1363);
- 3.18.22 destruction of an energy facility (18 U.S.C. 1366(a));
- 3.18.23 Presidential and Presidential Staff assassination and kidnapping (18 U.S.C. 1751(a), (b), (c), or (d));
- 3.18.24 acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air (18 U.S.C. 1992);
- 3.18.25 destruction of national defense materials, premises, or utilities (18 U.S.C. 2115; 18 U.S.C. 2156);
- 3.18.26 violence against maritime navigation (seizing a ship by force, destroying a ship or damaging its navigation systems) (18 U.S.C. 2280);
- 3.18.27 violence against maritime fixed platforms (an artificial island, installation or structure permanently attached to the sea-bed for the purpose of exploration or exploitation of resources or for other economic purposes (18 U.S.C. 2281);
- 3.18.28 homicides and other violence against U.S. nationals occurring outside of the United States (18 U.S.C. 2332);
- 3.18.29 the use of weapons of mass destruction (18 U.S.C. 2332a);
- 3.18.30 acts of TERRORISM transcending national boundaries (18 U.S.C. 2332b);
- 3.18.31 bombing of public places and facilities (18 U.S.C. 2332f);
- 3.18.32 producing, transferring, or threatening to use missile systems designed to destroy aircraft (18 U.S.C. 2332g);
- 3.18.33 producing, transferring, or threatening to use radiological dispersal devices (18 U.S.C. 2332h);
- 3.18.34 harboring TERRORISTS (18 U.S.C. 2339);
- 3.18.35 providing material support to TERRORISTS (18 U.S.C. 2339A);
- 3.18.36 providing material support to terrorist organizations (18 U.S.C. 2339B);
- 3.18.37 financing TERRORISM (18 U.S.C. 2339C);
- 3.18.38 receiving military-type training from a FTO (18 U.S.C. 2339D);
- 3.18.39 torture (18 U.S.C. 2340A);
- 3.18.40 developing, transferring, possessing, or threatening to use atomic weapons (42 U.S.C. 2122);

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 3.18.41 sabotage of nuclear facilities or fuel (42 U.S.C. 2284);
- 3.18.42 aircraft piracy (49 U.S.C. 46502);
- 3.18.43 assault on a flight crew with a dangerous weapon (49 U.S.C. 46504);
- 3.18.44 carrying a weapon or explosive aboard an aircraft (49 U.S.C. 46505(b) or (c); 49 U.S.C. 46506 if homicide or attempted homicide is involved);
- 3.18.45 damaging or destroying an interstate gas pipeline facility, an interstate hazardous liquid pipeline facility, or either an intrastate gas pipeline facility or intrastate hazardous liquid pipeline facility (49 U.S.C. 60123(b)); or
- 3.18.46 manufacturing, distributing, or possessing controlled substances intending to provide anything of pecuniary value to a FTO, member, or group (Section 1010A (iv) of the Controlled Substances Import and Export Act).

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## CHAPTER 4: NO FLY, SELECTEE AND EXPANDED SELECTEE LISTS IMPLEMENTATION GUIDANCE

### I. BACKGROUND

- 4.1 On October 21, 2004, the Deputies Committee established the criteria for the No Fly and Selectee Lists. On January 10, 2005, the DHS released the No Fly and Selectee Lists Implementation Guidance (Implementation Guidance) to provide direction on how to implement the No Fly and Selectee List criteria. The Implementation Guidance was updated and supplemented on July 25, 2006.
- 4.2 On February 8, 2008, the Deputies Committee approved the addition of a third and fourth criterion to the No Fly List. The Terrorist Screening Center Policy Board Working Group<sup>69</sup> revised the Implementation Guidance on March 5, 2008, to provide direction on how to implement these new criteria.
- 4.3 Following the attempted TERRORIST attack on December 25, 2009, the President directed that a review of the current No Fly and Selectee List criteria be conducted and recommendations be made regarding whether any adjustments were needed. The Terrorist Screening Center Policy Board Working Group, in conjunction with the Information Sharing Access IPC, recommended certain changes in the lists' criteria and implementation guidance. Those recommendations were approved by the Deputies Committee on July 16, 2010.

### II. PRE-CONDITIONS FOR PLACEMENT ON THE NO FLY OR SELECTEE LIST

- 4.4 Generally, in order to be included on either the No Fly or Selectee List, two pre-conditions must both be met:
  - 4.4.1 **Minimum Identifying Criteria.** Absent a Special Situation as described below<sup>70</sup>, minimum identifying biographic criteria consisting of First Name, Last Name, Full Date of Birth are required; and,
  - 4.4.2 **Minimum Substantive Derogatory Criteria.** The minimum substantive derogatory criteria for inclusion must be met.<sup>71</sup>

---

<sup>69</sup> This Working Group included representatives from Department of State, Department of Justice, Department of Homeland Security, Federal Bureau of Investigation, Central Intelligence Agency, Transportation Security Administration, National Counterterrorism Center, Terrorist Screening Center, Department of Treasury, and U.S. Customs and Border Protection.

<sup>70</sup> See Chapter 4, Section IX, for additional information regarding the full date of birth requirement and applicable exceptions.

<sup>71</sup> See Paragraph 1.58 for expedited nominations procedures.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

### III. NO FLY LIST CRITERIA

4.5 Any person, regardless of citizenship, who represents:

4.5.1 a threat of committing an act of "international TERRORISM" (as defined in 18 U.S.C. 2331(1)) or "domestic TERRORISM" (as defined in 18 U.S.C. 2331(5)) with respect to an aircraft (including a threat of air piracy, or a threat to airline, passenger, or civil aviation security); or,

4.5.2 a threat of committing an act of "domestic TERRORISM" (as defined in 18 U.S.C. 2331(5)) with respect to the homeland<sup>72</sup>; or,

4.5.3 a threat of committing an act of "international TERRORISM" (as defined in 18 U.S.C. 2331(1)) against any U.S. Government facility abroad and associated or supporting personnel, including U.S. embassies, consulates and missions, military installations (as defined by 10 U.S.C. 2801(c)(4)), U.S. ships, U.S. aircraft, or other auxiliary craft owned or leased by the U.S. Government; or,

4.5.4 a threat of engaging in or conducting a violent act of TERRORISM and who is OPERATIONALLY CAPABLE<sup>73</sup> of doing so.

4.6 **Detainees at the Naval Station, Guantanamo Bay, Cuba.** Any individual who was a "detainee" held at the Naval Station, Guantanamo Bay, Cuba, unless the President certifies in writing to Congress that the detainee poses no threat to the United States, its citizens, or its allies. For purposes of this subparagraph, the term "detainee" means an individual in the custody or under the physical control of the United States as a result of armed conflict.<sup>74</sup>

### IV. FURTHER CLARIFICATION OF THE NO FLY CRITERIA

4.7 **Third No Fly List Criterion.** Prior to the addition of the third No Fly List criterion (see Paragraph 4.5.3), a concern over the breadth of the No Fly List arose when KNOWN or SUSPECTED TERRORISTS who posed a threat to a U.S. military base overseas did not meet the criteria for inclusion on the No Fly List. Despite national interests, the threat to the overseas military base did not involve either civil aviation (as set forth in the first No Fly List criterion) or an act of domestic TERRORISM to the homeland (as set forth in the second No Fly List criterion). "Domestic Terrorism" requires that a subject's TERRORIST ACTIVITIES occur primarily within the territorial jurisdiction of the United States. "Homeland" does not include bases and embassies located abroad. Even in those instances when the IC had identified a KNOWN or SUSPECTED TERRORIST'S specific target, KNOWN or SUSPECTED TERRORISTS maintained the advantage of operational flexibility. The third No Fly List criterion addresses

<sup>72</sup> Domestic acts of TERRORISM are those that primarily occur "within the territorial jurisdiction of the United States." See 18 U.S.C. 2331(5)(C).

<sup>73</sup> See Paragraph 4.8.2, *infra*, that defines "OPERATIONALLY CAPABLE."

<sup>74</sup> See 49 U.S.C. 44903(j)(2)(C)(v).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

this specific vulnerability and counters the ability of KNOWN or SUSPECTED TERRORISTS to target U.S. Government facilities outside of the "homeland" (e.g., the October 12, 2000 attack upon the U.S. Navy guided missile destroyer USS Cole while it was harbored in the Yemeni port of Aden).

#### 4.8 Fourth No Fly List Criterion.

4.8.1 **Enable Flexibility.** The fourth No Fly List criterion (*see* Paragraph 4.5.4) is intended to enable flexibility for nominations to the No Fly List of OPERATIONALLY CAPABLE KNOWN or SUSPECTED TERRORISTS who pose a threat of committing an act of international TERRORISM abroad, but who do not meet the first, second or third No Fly List criterion because they do not pose a threat to civil aviation, a threat to the homeland, or a threat to U.S. facilities and their associated or supporting personnel. Previously, the No Fly List criteria did not prevent KNOWN or SUSPECTED TERRORISTS from traveling aboard aircraft, even though they may have had the intent and OPERATIONAL CAPABILITY to commit a TERRORIST act against U.S. nationals abroad (outside of the "homeland") or against a target with no nexus to the United States or its nationals. The fourth No Fly List criterion now addresses these two vulnerabilities.

4.8.2 **OPERATIONALLY CAPABLE Defined.** An individual is "OPERATIONALLY CAPABLE" if, based on credible intelligence, he or she, acting individually or in concert with others, reasonably appears to have the ability, knowledge, opportunity, and intent or is actively seeking the opportunity to engage in a violent act of TERRORISM consistent with 18 U.S.C. 2331 or 18 U.S.C. 2332b. For example, attempting to obtain an IED would indicate an individual is OPERATIONALLY CAPABLE of committing an act of TERRORISM. However, simply conducting internet research concerning IEDs would not be sufficient without additional activity. Depending on the circumstances, and in combination with other facts, scouting potential targets or traveling for no legitimate purpose to places that have TERRORIST training grounds, regardless of whether the person is presently capable of using an IED, might also indicate an individual is OPERATIONALLY CAPABLE of committing an act of TERRORISM.

4.8.3 **Possible Indicators of Being OPERATIONALLY CAPABLE.** In determining whether an individual is OPERATIONALLY CAPABLE, consideration should be given to the following indicators regarding ability, knowledge, opportunity, and/or intent:

- 4.8.3.1 Subject has undergone TERRORIST training or been provided some instruction, to include receiving military training by a designated terrorist group;
- 4.8.3.2 Subject has indicated intent to participate in planning/conducting an attack;
- 4.8.3.3 Subject has expressed desire to martyr him/herself;
- 4.8.3.4 Subject is in repeated contact with a KNOWN TERRORIST facilitator who recruits or facilitates travel of operatives;
- 4.8.3.5 Subject is planning an attack either alone or as part of a group; or,

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

4.8.3.6 Subject is associated with a TERRORIST group/cell and the subject is accumulating weapons/explosives.

4.9 **OPERATIONALLY CAPABLE Scenarios.** The three scenarios set forth below serve as some examples of No Fly List nominations that would fall under the fourth No Fly List criterion:

4.9.1 There is credible information that the planning or preparation for a TERRORIST attack against the interests of the United States or a foreign government is ongoing and there is an indication that an individual is OPERATIONALLY CAPABLE;

4.9.2 There is credible information that an individual is linked with an organization known to target U.S. interests. The actual target may be unknown but indicated to be a commercial facility frequented by U.S. citizens abroad. Intelligence identifies an operational or pre-operational capability of this individual whose cell is planning a near-term attack on a target (e.g., a plot to kill U.S. nationals residing in a foreign hotel or frequenting a foreign nightclub); or,

4.9.3 There is credible information that an individual is linked with an organization known to target foreign governments. The actual target may be unknown but indicated to be a foreign government facility such as an embassy, consulate, mission or military installation. Intelligence identifies an operational or pre-operational capability of this individual whose cell is planning a near-term attack on a target (e.g., a plot to bomb the British Parliament or the March 11, 2004, Madrid bombing).

**4.10 One-Time Waiver Policy.**

4.10.1 TSA regulations prohibit U.S. flagged air carriers and foreign flagged air carriers from transporting individuals, who pose the level of threat required for No Fly status, on regulated commercial flights, including all flights operated by U.S. air carriers regardless of the location, and flights operated by foreign air carriers to, from, or over the United States. This prohibition applies regardless of the individual's status as a U.S. PERSON.

4.10.2 When necessary, the U.S. Government may authorize and grant a One Time Waiver (OTW) to an air carrier permitting the carrier to transport an individual on a specified itinerary under controlled conditions. OTWs are coordinated with DHS (including CBP and TSA), FBI, DOS and DOJ as appropriate, prior to being authorized by TSC. Once authorized by TSC, TSA will review the conditions of transport and may grant the waiver, permitting the air carrier to transport the individual. If the itinerary changes, or the conditions of transport of the individual change, TSA will deny boarding to the individual until such time as satisfactory conditions are present.

**4.10.3 U.S. PERSONS Encountered Overseas.**

4.10.3.1 While placement on the No Fly List does not legally bar a U.S. PERSON from

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

returning to the United States, the U.S. Government has adopted a policy to review all cases in which a U.S. PERSON on the No Fly List is denied boarding on a commercial flight bound for the United States to determine whether an OTW may be appropriate. TSC will initiate this assessment immediately, and may approve an OTW in advance. TSA will not review or authorize an OTW until such time as an acceptable itinerary is available.

- 4.10.3.2 In order to facilitate communication with such an individual, the U.S. Government has determined, as a matter of policy, that U.S. Citizens denied boarding on a commercial flight returning to the United States should be referred to the consular section of the nearest U.S. Embassy or Consulate, which will facilitate communication with the individual, including providing the individual with instructions in the event an OTW is authorized. In keeping with the U.S. Government's traditional policy of neither confirming nor denying whether an individual is on the Terrorist Watchlist, the individual is not informed of his or her watchlist status or that he or she would be traveling under a waiver.

## V. SELECTEE LIST CRITERIA

- 4.11 **Selectee List Criteria.** Any person regardless of citizenship, who does not meet the criteria for inclusion on the No Fly List and who:

- 4.11.1 is a member of a foreign or domestic TERRORIST organization<sup>75</sup> (including a "foreign TERRORIST organization" designated pursuant to Statute or Executive Order, as described in Paragraph 3.11.2); and,
- 4.11.2 is associated with "TERRORIST ACTIVITY" (as such term is defined in section 212(a)(3)(B) of the INA [8 U.S.C. 1182(a)(3)(B)]); unless information exists that demonstrates that the application of secondary screening to such person is not necessary, in which case such persons may be excluded from the Selectee List.

## VI. EXPANDED SELECTEE LIST CRITERIA

- 4.12 The Expanded Selectee List (ESEL) includes records in the TSDB that contain a full name and full date of birth, regardless of the citizenship of the subject, who do not meet the criteria to be placed on either the No Fly or Selectee Lists, excluding exceptions to the REASONABLE SUSPICION standard.

## VII. ACTIONS BASED UPON POSITIVE MATCHES TO THE NO FLY, SELECTEE, OR EXPANDED SELECTEE LISTS

<sup>75</sup> Members of a defunct terrorist group are included in this criterion if the person was a member of the group when it participated in TERRORIST ACTIVITY.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- 4.13 The actions resulting from inclusion on the No Fly, Selectee, or Expanded Selectee List are generally as follows:
- 4.13.1 Individuals that are POSITIVE MATCHES to the No Fly List are prohibited from boarding an aircraft;
  - 4.13.2 Individuals that are POSITIVE MATCHES to the Selectee List undergo enhanced screening prior to boarding an aircraft;
  - 4.13.3 Individuals that are POSITIVE MATCHES to the Expanded Selectee List undergo enhanced screening prior to boarding an aircraft.
- 4.14 Selectee, Expanded Selectee, and random screening all result in the same operational response of receiving enhanced screening by Transportation Security Officers prior to boarding an aircraft. TSA will notify the TSC of all No Fly, Selectee, and Expanded Selectee ENCOUNTERS.

**VIII. IMPLEMENTATION GUIDELINES**

- 4.15 **General Guidelines.** The watchlisting community has developed six general guidelines regarding the No Fly and Selectee Lists that should be reemphasized in order to effectively implement the No Fly List and Selectee List criteria. The six general guidelines are:
- 4.15.1 When evaluating the significance, relevance and validity of a threat, careful consideration should be given to the extent to which the threat is current, specific and credible.
  - 4.15.2 The Selectee List is not a default position for those who do not qualify for inclusion on the No Fly List and has distinct elements that must be met before an individual may be included.
  - 4.15.3 The purpose of the No Fly List is to protect against acts of TERRORISM; inclusion on the No Fly List has consequences that are operational, legal, economic, and diplomatic.
  - 4.15.4 Except for expedited nominations made pursuant to Paragraph 1.58 of the Watchlisting Guidance, the decision to include a person on the No Fly List or Selectee List must include substantive DEROGATORY INFORMATION that satisfies the aforementioned criteria and thus justifies inclusion on either list. In cases where nominations contain no substantive DEROGATORY INFORMATION, or contain insufficient substantive DEROGATORY INFORMATION, the individual will not be included on either the No Fly List or Selectee List.
  - 4.15.5 In accordance with determinations made pursuant to Paragraph 1.59 of the Watchlisting Guidance, the White House may direct the TSC to place categories of individuals on the No Fly List or the Selectee List on a temporary basis based on current

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

and credible intelligence information or a particular threat stream that indicates a certain category of individuals may conduct an act of domestic or international TERRORISM.

- 4.15.6 Under exigent operational circumstances, when DEROGATORY INFORMATION may not be widely disseminated or stored in TIDE, individual watchlist status determinations can be made by the Director of the TSC, in accordance with the relevant criteria<sup>76</sup> contained in the Watchlisting Guidance. Coordination should occur with relevant NOMINATING AGENCIES and SCREENERS.

- 4.16 **Totality of the Information.** The foregoing guidance is neither intended to be determinative nor intended to serve as a checklist. Rather, it is intended to guide the watchlisting community in assessing whether the established criteria are satisfied for a specific record, based on the totality of available information, a current threat stream, and/or the current threat environment.

**IX. SPECIAL SITUATIONS<sup>77</sup>**

- 4.17 **Requirement for Full Names and Complete Dates of Birth.** Generally, TERRORIST identities nominated to either the No Fly or the Selectee List must have both a full name and a complete date of birth. Identities without both will usually not be included on either list. Dates of birth shall not be fabricated.<sup>78</sup>

- 4.17.1 There is, however, a narrow exception to the requirement for full names and complete dates of birth for individuals from non-Visa Waiver Program countries for international TERRORIST nominations. If a non-Visa Waiver Program country<sup>79</sup> has issued a travel document with only a year of birth, or a verified government-issued identification document with only a year of birth, then it is permissible to use only that year of birth. The NOMINATING AGENCY, however, should, whenever possible, specify the type of document containing the year of birth, and the passport number (if the document is a passport). Otherwise, a year of birth alone will not be accepted for nominations to the No Fly or Selectee Lists. The NOMINATING AGENCY has a continuing obligation to attempt to determine the complete date of birth.

- 4.18 **Expedited Waiver of "Full Date of Birth" Requirement for No Fly or Selectee Nominations.** When necessitated by exigent circumstances, a NOMINATOR may nominate an individual or individuals to the No Fly or Selectee List with only a partial date of birth, but for whom there is additional identifying information. This provision is intended to enable nominations based on current and credible intelligence information or a particular threat

<sup>76</sup> Determinations made under this section apply to the No Fly, Selectee and Expanded Selectee List criteria.

<sup>77</sup> See Paragraph 1.59 for a complete discussion of expedited nomination procedures for temporary, threat-based categories.

<sup>78</sup> The dates of birth of January 1 (01/01/xxxx), July 1 (07/01/xxxx), November 11 (11/11/xxxx), and December 31 (12/31/xxxx) are examples of dates that may be fabricated and as such, should receive additional scrutiny at all stages of the reporting, nomination, and watchlisting process.

<sup>79</sup> Visa Waiver Program countries include a complete date of birth in their passports.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

stream that indicates the subject(s) may be used to conduct an act of domestic or international terrorism as defined in 18 U.S.C. 2331(1), or as a Federal crime of terrorism as defined in 18 U.S.C. 2332b(g)(5). The goal of this provision is to fashion a watchlisting response that is appropriate to the nature, specificity, and severity of the threat. To achieve this goal, in addition to the credibility of the threat intelligence, due consideration should be given to:

- 4.18.1 The harm to public safety posed by the threat;
  - 4.18.2 The clarity and specificity of the information giving rise to the threat as to time, place, method, and identity of the suspected perpetrator(s);
  - 4.18.3 The anticipated impact on international and domestic travel, civil liberties, and foreign relations; and,
  - 4.18.4 The best available screening tools, other than the No Fly or Selectee Lists, given the type and specificity of identifiers and travel data.
- 4.19 This waiver should be utilized in limited circumstances when extreme DEROGATORY INFORMATION has been identified demonstrating the threat. The waiver should be valid as long as the threat remains.

**X. NOMINATIONS THAT ARE INELIGIBLE/NOT SUITABLE FOR EITHER THE NO FLY OR THE SELECTEE LIST<sup>80</sup>**

- 4.20 Nominations based on exceptions to the minimum substantive derogatory criteria contained in Paragraph 3.14, including immediate family members of TERRORISTS (*i.e.*, spouses or children of a KNOWN or SUSPECTED TERRORIST)<sup>81</sup> are ineligible/not suitable for inclusion on either the No Fly or Selectee List, absent independent DEROGATORY INFORMATION;
- 4.21 Subjects of lost or stolen passports or travel documents are ineligible/not suitable for inclusion on either the No Fly or Selectee List, absent independent DEROGATORY INFORMATION;
- 4.22 Deceased individuals are ineligible for inclusion on either the No Fly or Selectee List unless they meet the exceptions set forth in Paragraph 3.17, Identities of Deceased Individuals.

---

<sup>80</sup> This section can be overridden in the event of an expedited, threat-based categorical nomination procedures, pursuant to Paragraph 1.59.

<sup>81</sup> See INA § 212(a)(3)(B)(i)(IX)[8 U.S.C. 1182(a)(3)(B)(i)(IX)].

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## CHAPTER 5: ENCOUNTER MANAGEMENT AND ANALYSIS

## I. INTRODUCTION AND PURPOSE

5.1 This guidance addresses the collection, processing, and analysis of TERRORISM INFORMATION collected by the SCREENERS during an ENCOUNTER with a watchlisted subject. As described below, all information gathered during an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST<sup>82</sup> is referred to as an ENCOUNTER PACKAGE. This guidance does not create any new authorities for the collection of any information during ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS. Rather, it identifies the types of information that a Department or Agency should consider collecting during an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST if it possesses the authority to collect such information, and should share with the interagency community consistent with their legal authorities and executive policy.<sup>83</sup>

## 5.2 Definitions.

5.2.1 ENCOUNTER. An ENCOUNTER is defined as an event in which an individual is identified during a screening process to be a "POSITIVE MATCH," "POTENTIAL MATCH," or "INCONCLUSIVE MATCH," to an individual who has been designated in the TSDB as a KNOWN or SUSPECTED TERRORIST. An ENCOUNTER can be a face-to-face meeting with a KNOWN or SUSPECTED TERRORIST, electronic or a paper-based ENCOUNTER (e.g., the KNOWN or SUSPECTED TERRORIST has submitted an application for a benefit like a visa, Electronic System for Travel Authorization (ESTA) application, or information is provided to the United States by a foreign government, aircraft operator, or other private entity). Chapter 5 is only concerned with POSITIVE MATCHES, which occur when the TSC determines that information about a subject encountered by a SCREENER matches a TSDB record.

5.2.2 TERRORISM INFORMATION. TERRORISM INFORMATION in this chapter includes purely domestic terrorism as defined in the TSC MOU and incorporates the definition found in section 1016 of the IRTPA (6 U.S.C 485), as amended. The term "TERRORISM INFORMATION" means —

5.2.2.1 all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

5.2.2.1.1 the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or

<sup>82</sup> Sharing information for reasons not related to KNOWN or SUSPECTED TERRORIST categories should be limited to updating biographic identifiers, and the sharing of relevant information that may assist in making decisions related to a change in a person's status in the TSDB and/or TERRORISM INFORMATION.

<sup>83</sup> Obligations include those imposed by IRTPA section 1021 or by interagency agreement (e.g., the *Information Sharing MOU* (Appendix 5), the *TSC MOU* (Appendix 3) and Addendum B to the *TSC MOU* (Appendix 4)).

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

individuals involved in transnational TERRORISM;

5.2.2.1.2 threats posed by such groups or individuals to the United States, U.S. PERSONS, or U.S. interests, or to those of other nations;

5.2.2.1.3 communications of or by such groups or individuals; or,

5.2.2.1.4 groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

5.2.2.2 includes weapons of mass destruction information.

5.2.2.2.1 **Weapons of Mass Destruction Information.** Information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a TERRORIST or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a TERRORIST or a terrorist organization against the United States.

## II. PROCESSING TERRORISM INFORMATION FROM ENCOUNTERS WITH POSITIVELY IDENTIFIED KNOWN OR SUSPECTED TERRORISTS

5.3 This section describes the major types of ENCOUNTERS by various Departments and Agencies. ENCOUNTER PACKAGES obtained from a KNOWN or SUSPECTED TERRORIST ENCOUNTER will be processed as follows:

5.4 **Department of Homeland Security ENCOUNTERS.** DHS has more ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS than any other U.S. Government component. The descriptions below provide information for the majority of DHS ENCOUNTERS, although it is not an exhaustive list of ENCOUNTER opportunities or the types of TERRORISM INFORMATION available for collection. When lawful and available, both biographic and biometric information will be collected as part of the ENCOUNTER PACKAGE.

5.4.1 **U.S. Customs and Border Protection.** CBP ENCOUNTERS occur at ports of entry (POE), between POEs, or at the last point of departure to the United States at foreign airports through CBP programs like Pre-Clearance and the Immigration Advisory Program (IAP). Information available for collection from these ENCOUNTERS may include, but is not limited to, pocket litter, travel information, identification documents, travel companions, legal documents, and other information gathered during interviews and the examination process. CBP receives international travel reservation information of KNOWN or SUSPECTED TERRORISTS for commercial air travel to and from the United States (which may include travel companion information) and international private and

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

commercial flight manifests, as well as, commercial vessel manifest for travel to and from the United States. With the exception of passenger information required by law to be transmitted to DHS prior to a passenger's arrival, most information is generally collected by CBP when the person is interviewed or apprehended. The National Targeting Center – Passenger (NTC-P) and NTC-Cargo (NTC-C) are CBP entities responsible for communicating with the TSC regarding ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS, to include providing relevant ENCOUNTER information.<sup>84</sup> NTC-P and NTC-C also provide a copy of the examination results to the TSOU for dissemination to the appropriate investigating Agencies.

**5.4.2 Transportation Security Administration.** TSA generally encounters KNOWN or SUSPECTED TERRORISTS through screening commercial aircraft passengers against subsets of the TSDB and during the application process for a credential or benefit in the transportation or critical infrastructure environment (e.g., Transportation Worker Identification Credential (TWIC)). When an airline encounters subjects who are possible matches to the No Fly or Selectee List, the air carriers are required to supply the passenger's name and one piece of identifying data (in the form of a government-issued photo identification that contains a date of birth) to the TSA's Office of Intelligence and Analysis (OIA). TSA OIA submits that information, along with information regarding the carrier, flight number, time of departure, and destination to the TSC.

**5.4.2.1** Absent an arrest warrant, or unless probable cause arises during the ENCOUNTER, SCREENERS are reminded that **placement on the No Fly or Selectee List is not a legal basis to detain a KNOWN or SUSPECTED TERRORIST.** To the extent legal authority exists to question a KNOWN or SUSPECTED TERRORIST, encounters with No Fly subjects at the airport may provide an additional opportunity to lawfully obtain ENCOUNTER PACKAGE information. For No Fly subjects who have made a domestic reservation, DHS will notify TSC in advance as well as when the No Fly subject presents at the airport ticket counter. TSC will then notify the TSOU who will notify both the FBI case agent and the airport liaison agent to coordinate the appropriate operational response.

**5.4.2.2** For KNOWN or SUSPECTED TERRORIST ENCOUNTERS as a result of an individual applying for a TSA benefit or credential, ENCOUNTER PACKAGE information can include any supporting documents or information collected as a part of the application process. The ENCOUNTER, and any corresponding information, is communicated to the TSC and other Government Agencies, as appropriate through TSA OIA.

**5.4.3 United States Citizenship and Immigration Services.** U.S. Citizenship and Immigration Services (USCIS) interact with millions of individuals every year and

---

<sup>84</sup> CBP may also encounter such individuals in the course of processing an application and/or conducting an interview of an applicant for a trusted traveler program (e.g., NEXUS, Free and Secure Trade (FAST), Global Entry, SENTRI, etc.).



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

ENCOUNTERS KNOWN or SUSPECTED TERRORISTS who file petitions or applications for immigration benefits internationally and domestically.<sup>85</sup> The USCIS official contacts the TSC to report an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST. Before making a decision on the immigration application or benefit, USCIS contacts the ORIGINATOR/NOMINATOR to obtain additional information that may help determine whether the individual is eligible or ineligible to receive the immigration benefit. In such cases, USCIS seeks further information from the record owner or case agent and may seek de-classification of information relating to the application. In addition, USCIS contacts the ORIGINATOR/NOMINATOR to discuss whether the USCIS decision to grant or deny the application or benefit would interrupt or negatively affect any ongoing investigation.

5.4.3.1 USCIS maintains a presence at law enforcement and intelligence Agency entities to further information sharing regarding KNOWN or SUSPECTED TERRORISTS. USCIS maintains information, including the subject's Alien File (A-File) and other records. The type of information that may be contained in USCIS files, including the A-File, could be biometric data (fingerprints and photographs); identity documents; information relating to the application; addresses, as well as family and work history information; immigration benefit application information; and records of previous ENCOUNTERS that DHS has had with the subject. Other SCREENERS — as well as other appropriate organizations who are considering nominating a potential KNOWN or SUSPECTED TERRORIST or who have ENCOUNTERS with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST— are advised that they can request, on a case-by-case basis, a copy of the KNOWN or SUSPECTED TERRORIST's A-File from USCIS if the KNOWN or SUSPECTED TERRORIST has applied for immigration or citizenship benefits.<sup>86</sup>

5.4.4 **U.S. Immigration and Customs Enforcement.** Immigrations and Customs Enforcement (ICE) is the principal investigative arm of DHS. ICE is also the federal law enforcement organization responsible for immigration and customs-related investigations and detention within the interior and at the borders of the United States. ICE frequently ENCOUNTERS potential KNOWN or SUSPECTED TERRORISTS during enforcement activities under its purview. Such ENCOUNTERS are documented within ICE Enforcement and Removal Operations (ERO) via the Known Suspected Terrorist Encounter Protocol and reported to the TSC and ICE's Homeland Security Investigations (HSI). ICE HSI Special Agents frequently encounter KNOWN or SUSPECTED TERRORISTS internationally, domestically, at U.S. POEs, and when KNOWN or SUSPECTED TERRORISTS are the subjects of an ICE investigation. These ENCOUNTERS are

<sup>85</sup> For example, a U.S. PERSON who is a KNOWN or SUSPECTED TERRORIST may file a petition for a foreign national or a U.S. PERSON who is not a KNOWN or SUSPECTED TERRORIST may file a petition for a foreign national who is a KNOWN or SUSPECTED TERRORIST.

<sup>86</sup> Because USCIS is the custodian of information acquired through the immigration process relating to an individual and because the A-File is not routinely attached to the TSDB or TIDE, a specific request to USCIS is necessary in order to obtain information from the A-File.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

documented by HSI Special Agents in Reports of Investigation (ROI). All ROIs documenting ENCOUNTERS/interviews with a KNOWN or SUSPECTED TERRORIST are shared with the IC.

5.4.4.1 In addition, under section 428 of the Homeland Security Act, the Secretary of Homeland Security has the authority to refuse visas in accordance with the law and to assign employees of DHS to diplomatic and consular posts to review visa applications and conduct investigations.<sup>87</sup> ICE, through the Visa Security Program, exercises this authority. Reviews of visa applications and interviews with applicants can result in the encounter of KNOWN or SUSPECTED TERRORISTS, facilitators, and associates as well as reveal previously unknown information relating to KNOWN or SUSPECTED TERRORISTS. HSI personnel assigned to the Visa Security Program, and to U.S. Embassies and Consulates abroad, work closely with their DOS counterparts to identify KNOWN or SUSPECTED TERRORISTS and report findings through established processes. Finally, ICE may encounter KNOWN or SUSPECTED TERRORISTS awaiting immigration hearings who are housed in service processing/detention centers. These detention facilities can document interactions with the aliens while they are detained in the facility, as well as document materials found on the individual at the time of processing. For all immigration and enforcement activities, ICE will communicate with the TSC regarding encounters with watchlisted individuals, and will submit relevant ENCOUNTER information to the TSC.

5.4.5 **United States Coast Guard.** The U.S. Coast Guard's Coastwatch branch screens crew and passenger information on vessel manifests, which are required by regulation to be transmitted to the National Vessel Movement Center (NVMC) prior to a vessel's arrival in a U.S. port. Coastwatch communicates with the NTC-P and TSC regarding any KNOWN or SUSPECTED TERRORIST ENCOUNTERS during this process. The Coast Guard physically encounters few KNOWN or SUSPECTED TERRORISTS, and such ENCOUNTERS could occur from random and regular inspections of vessels and port facilities, ship boardings, investigations, or Coast Guard licensing activities. The type of information available for collection is dependent on the type of ENCOUNTER. The ENCOUNTER, and any corresponding information, is communicated to the TSC through Coast Guard Office of Intelligence and Criminal Investigations. Based on the encountering situation, intelligence reporting will be written to provide situational awareness to the IC.

5.4.6 **United States Secret Service.** Although United States Secret Service (USSS) does not encounter many KNOWN or SUSPECTED TERRORISTS, such ENCOUNTERS usually involve KNOWN or SUSPECTED TERRORISTS with a domestic nexus to TERRORISM. Such encounters can be the result of investigations or for event screening (e.g., National Security Special Events, political events, large scale sporting events). These

---

<sup>87</sup> Consistent with section 428 of the Homeland Security Act and the *Memorandum of Understanding between the Secretaries of State and Homeland Security Concerning Implementation of Section 428 of the Homeland Security Act of 2002*, the Secretary of Homeland Security may direct a consular officer to refuse or revoke a visa.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

ENCOUNTERS will be coordinated with the FBI, who will handle them as they do all other FBI KNOWN or SUSPECTED TERRORIST ENCOUNTERS.

**5.4.7 Department of Homeland Security Intelligence & Analysis.** DHS I&A provides end products and analytical reports, which are generally available to the NCTC and the broader counterterrorism analytic community, including fusion centers. DHS I&A works closely with DHS components to ensure non-traditional streams of information are fused with traditional sources of information from other members of the IC to give a complete picture of potential threats to the nation. DHS I&A "connects the dots" for intelligence reporting and ENCOUNTERS of the DHS components, and as such, has limited opportunity for ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS.

**5.5 Department of State ENCOUNTERS.** For DOS ENCOUNTERS with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST, the DOS unit at the TSC will do the following:

**5.5.1 Visa Applications.** DOS/TSC will upload the electronic visa application from the CCD to the individual's EMA record. DOS/TSC will coordinate with the overseas posts to scan in CCD all other available DOS documents associated with the individual. DOS information about whether a visa is issued is currently available in individual case records in the CCD; DOS is currently investigating upgrades to the CCD's report function that will make the visa decision data more easily accessible to TSC and other users.

**5.5.2 Visa Revocations.** DOS/TSC will upload the electronic visa application from the CCD to the individual's EMA record.

**5.5.3 Passports.** After encounters with KNOWN or SUSPECTED TERRORISTS possessing passports issued by the United States, the TSOC will upload the Passport Information Electronic Records System (PIERS) application forms from the CCD to the individual's EMA record. DOS/TSC will coordinate with the overseas posts to scan in CCD all other available DOS documents associated with the individual.

**5.6 United States Agency for International Development ENCOUNTERS.** United States Agency for International Development (USAID) works in agriculture, democracy and governance, economic growth, the environment, education, health, global partnerships, and humanitarian assistance in more than 100 countries. When USAID receives an application seeking financial assistance, prior to granting, these applications are subject to vetting by USAID intelligence analysts at the TSC. If USAID/TSC finds that an application relates to a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST in the TSDB, USAID/TSC will provide any TERRORISM INFORMATION concerning the application and follow standard TSC procedures for processing TERRORISM INFORMATION, to include logging the ENCOUNTER in EMA.

**5.7 Foreign Partner ENCOUNTERS.** After each ENCOUNTER by a foreign partner, DOS/TSC will ask the respective country for the subject's photo, additional biographic data and any

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

TERRORISM INFORMATION on the ENCOUNTER Information List gathered during the ENCOUNTER. Provision of any material collected by the foreign partner depends on the arrangement with, and legal authorities of, the particular foreign partner involved. Therefore, gathering and sharing this TERRORISM INFORMATION will be done on a case-by-case, country-by-country basis.

**5.8 Federal Bureau of Investigation/Law Enforcement ENCOUNTERS.** These ENCOUNTERS can be subdivided into three categories:

**5.8.1 Name-Based Queries.** Name-based transaction queries by law enforcement personnel (e.g., traffic stops) made to the FBI's National Crime Information Center at the Criminal Justice Information Services (CJIS) Division that match a name in the KSTF (a sub-file of NCIC) are deemed to be POTENTIAL MATCHES. They are routed electronically to TSC for confirmation and subsequent processing as an ENCOUNTER.

**5.8.2 Fingerprint-Based Queries.** Fingerprint-based queries submitted for criminal identification purposes (e.g., an arrest/booking) or for civil identification purposes (e.g., an employment background check) are made to the Integrated Automatic Fingerprint Identification System (IAFIS). For POSITIVE MATCHES to records flagged as KNOWN or SUSPECTED TERRORIST records, the CJIS Division's Special Identities Unit notifies the TSC and the FBI case agent (or the Agency that identified the subject as a possible TERRORIST). In similar fashion, CJIS Division's Global Initiatives Unit coordinates positive fingerprint hits from its foreign submissions with the Legal Attaché. It should be noted that IAFIS and NCIC are separate systems that are not fully synchronized at the present time.

**5.8.3 National Instant Criminal Background Check System.** All background checks resulting from attempts to buy firearms or to obtain explosive permits submitted to the National Instant Criminal Background Check System (NICS) at CJIS are run against the KSTF. The TSC is immediately notified of all KSTF "hits." NICS consults with TSC to confirm the POSITIVE MATCHES and the FBI case agent to determine whether there is available information about the prospective purchaser to disqualify him or her from possessing a firearm or explosive as a matter of law. Regardless of whether the purchase is denied or permitted to proceed, all available information is obtained and provided to the TSC and, in turn, CTD, as TERRORISM INFORMATION and processed as an ENCOUNTER.

**5.9 Department of Defense ENCOUNTERS.** The Department of Defense (DoD) has force protection, operational capture/apprehend, and intelligence responsibilities and on occasion encounters KNOWN or SUSPECTED TERRORISTS. To the extent DoD knowingly encounters a KNOWN or SUSPECTED TERRORIST, DoD will report the ENCOUNTER in intelligence channels or to the FBI in cases described in the MOU between the FBI and DoD Governing Information Sharing, Operational Coordination and Investigative Responsibilities signed August 2, 2011 where the FBI is the lead. In cases where the FBI is not the lead for the ENCOUNTER, the

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

Defense Intelligence Agency (DIA) will be responsible for providing extracted information from the ENCOUNTER to NCTC via standard DIA national TERRORIST watchlisting procedures, which utilize community accepted standards. DoD law enforcement ENCOUNTERS will be handled in accordance with established law enforcement standards that provide notification to the FBI.

- 5.10 **All other Departments or Agencies.** Any other Department or Agency that has TERRORISM INFORMATION from an ENCOUNTER will contact the TSC/TSOC at 866-██████ to arrange a mutually acceptable transmission method.

### **III. CATEGORIES OF TERRORISM INFORMATION FROM ENCOUNTERS WITH POSITIVELY IDENTIFIED KNOWN OR SUSPECTED TERRORISTS OF POTENTIAL INTEREST**

- 5.11 **ENCOUNTER Information List.** The following ENCOUNTER Information List identifies categories of TERRORISM INFORMATION from ENCOUNTERS with positively identified KNOWN or SUSPECTED TERRORISTS that are of potential interest to NOMINATORS, other counterterrorism analysts, or the watchlisting community. The items identified are not intended to be an exclusive or exhaustive list of what constitutes TERRORISM INFORMATION.

- 5.11.1 ENCOUNTER information identified for collection in Addendum B to the *TSC MOU*<sup>88</sup> when there is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST:

1. Photographs
2. Fingerprints
3. Pocket litter
4. Written data
5. Reports of TERRORISM INFORMATION

- 5.11.2 Additional items of potential interest when lawfully collected during an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST:

1. Contemporaneous reports including the impressions or observations recorded by an official involved in the ENCOUNTER:
  - a) Reason/circumstances of ENCOUNTER
  - b) ICE Intel Reports
  - c) FBI Reports of Investigations
  - d) CBP Incident Reports
  - e) CBP Secondary Exam Report
  - f) USCIS applications or petitions
  - g) Non-Immigrant Visa (NIV) Applications (including CCD notes)

<sup>88</sup> See Appendix 3, *TSC MOU*.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- h) State, Local, Tribal, Territorial Police Report
  - i) TSA OIA No Fly and Selectee Reports
  - j) TSA OIA ENCOUNTER Reports (Vetting Match Reports) on transportation workers and other populations vetted by TSA against the TSDB
  - k) Spot Reports
  - l) Suspicious Activity Reports
  - m) Impounded vehicle inventory
  - n) Any inventory record
  - o) Any pictures, video or recording of or from the actual ENCOUNTER
  - p) Biometric or biographic identifiers of traveling associates
2. Surveillance-related documents:
- a) Maps
  - b) Pictures
  - c) Visitor or site information
  - d) Plans or diagrams (e.g., architectural drawings, blueprints, schemas)
3. Context regarding areas of potential interest or possible targets of KNOWN or SUSPECTED TERRORIST interest:
- a) Information regarding any high profile events taking place in geographic area of ENCOUNTER
  - b) Any critical infrastructure sites near the geographic area of ENCOUNTER
  - c) Unique characteristics or facts about your domain/area of responsibility/geographic area of ENCOUNTER
  - d) Event tickets (e.g., sporting events, concerts, designated National Security Special events)
  - e) Building access passes, electronic cards, fobs, keys
4. Mode of transportation used by the person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST, along with identifying information:
- a) Vehicle information (e.g., Vehicle registration, Vehicle identification number (VIN), Title, Driver's license, Car insurance cards or information)
  - b) Pilot medical license
  - c) Pilot certificates
  - d) Aircraft registration
  - e) Marine registration
  - f) EZ Pass or electronic vehicle payment system
5. Travel-related information:
- a) Passport exit/entry stamps indicating places of travel
  - b) Any visa application or denial information from other countries

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- c) Travel itineraries
  - d) Tickets (*e.g.*, plane, train, boat)
  - e) Hotels (*e.g.*, reservation confirmation, receipts)
  - f) Rental cars (*e.g.*, reservation confirmation, agreement, receipts)
  - g) Reservation method (*e.g.*, via travel agency or travel website)
  - h) PNR data
  - i) Travel manifests
  - j) Luggage or baggage tags (*e.g.*, airport check-in tags, identification tags, lost bag bar code tags)
  - k) Claim checks
  - l) Storage locker keys
  - m) Shipping documents and receipts
  - n) Automated Identification System (AIS) information for maritime shipping
  - o) Foreign airport security check stickers or labels
  - p) Conference/seminar materials (*e.g.*, invitation, brochure, schedule)
6. Information about gold and jewelry worn by person at time of ENCOUNTER (*e.g.*, receipts)
7. General items information:
- a) Business cards
  - b) Phone numbers
  - c) Address books
  - d) Email addresses
  - e) Any cards with an electronic strip on it (hotel cards, grocery cards, gift cards, frequent flyer cards)
  - f) Pre-paid phone cards
  - g) Insurance cards
  - h) Medical/Health insurance information
  - i) Prescription information (*e.g.*, doctor, pharmacy information)
  - j) Sales receipts
  - k) Any additional biographic or biometric identifiers to enhance identity matching of associates or family members with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST (as well as associates or family members referenced in interviews or documents carried by a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST)
  - l) Copies of identification documents obtained during the ENCOUNTER with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST (*e.g.*, passports, Seaman's Papers, Airman Certificates, driver's licenses, state identification cards, and similar government identification documents)
  - m) Any computer, uniform resource locator (URL), or Internet protocol (IP) address information
  - n) Calendars/schedulers

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

8. Licenses, permits, membership cards, and application information:
  - a) Membership cards (including library cards)
  - b) Gun show applications, firearms license, concealed weapons permit, shooting club memberships
  - c) HAZMAT license
  - d) Explosives permit
9. Tools or equipment information:
  - a) Scuba gear
  - b) Multiple cell phones
  - c) Binoculars
  - d) Peroxide
  - e) Ammunition
  - f) Camping fuel tabs
  - g) Any dual use material that could be used for TERRORIST ACTIVITY
10. Financial information:
  - a) Check book/individual or loose checks, including cashier's checks
  - b) Bank account numbers
  - c) Credit cards, especially those issued by U.S. banks and carried by non- U.S. PERSONS
  - d) Tax records
  - e) Business financial records
  - f) Bank statements
  - g) Credit card or billing statements
  - h) Utility bills
  - i) Anything with an account number
  - j) Wire transfer information, including receipts from Money Service Businesses
  - k) Denominations of money being carried (*i.e.*, what country(ies) currency(ies) are they carrying), including, if possible, the serial numbers of currency carried
  - l) Automated teller machine (ATM) receipts
  - m) Ledgers
11. Electronic media/devices observed or copied:
  - a) Cell phone list and speed dial numbers
  - b) Laptop images
  - c) GPS
  - d) Thumb drives
  - e) Disks
  - f) iPod or MP3
  - g) PDAs (*e.g.*, Palm Pilots, Trios)
  - h) Kindle or iPad (electronic books)
  - i) Cameras
  - j) Video and/or voice recorders

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- k) Pagers
- l) Any electronic storage media
- 12. Employment information:
  - a) Pay stubs
  - b) Employment applications
  - c) Want ads
  - d) Employer correspondence
  - e) Access cards, badges
- 13. Professional papers/Academic information:
  - a) Resumes
  - b) Academic transcripts
- 14. Legal document information:
  - a) Birth certificates
  - b) Immigration and naturalization documents
  - c) Marriage licenses
  - d) Divorce decrees
  - e) Adoption papers
  - f) Living Wills
  - g) Last Will and Testament
  - h) Parking tickets
  - i) Speeding tickets
  - j) Property records (deeds)
  - k) Summons
  - l) Criminal documents or civil lawsuit information
- 15. Miscellaneous item information:
  - a) Long term storage facilities (*e.g.*, access keys, codes)
  - b) Social networking accounts (*e.g.*, Facebook, Twitter, MySpace, LinkedIn, ICQ)
  - c) Titles of books, DVD/CD, brochures being carried and their condition (*e.g.*, new, dog-eared, annotated, unopened, professional journals)
  - d) Letters, envelopes
  - e) Letters of Introduction
  - f) Animal information (*e.g.*, vet or chip information)

**IV. ENCOUNTER MANAGEMENT ACTIONS**

**5.12 Handling of ENCOUNTER PACKAGES.** This section outlines the processes for handling and sharing ENCOUNTER PACKAGES by SCREENERS, the TSC and NCTC.

**5.13 FBI/Law Enforcement ENCOUNTERS.** TSOU coordinates the U.S. Government's response to an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST. All collection of TERRORISM

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

INFORMATION during law enforcement ENCOUNTERS (e.g., traffic violations, investigations, arrests) are coordinated between the NOMINATING AGENCY and the ENCOUNTERING AGENCY via TSOU.

5.13.1 For domestic and international ENCOUNTERS with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST, TSOU will do the following: After receiving notification of an ENCOUNTER from the TSC, TSOU will disseminate and coordinate information to FBI operational entities and federal, state, and local law enforcement Agencies. TSOU simultaneously coordinates with the appropriate FBI Field Division(s) and Case Agent(s); Joint Terrorist Task Forces (JTTFs); Airport Liaison Agents and Attaches (ALAs); Legal Attachés (LEGATs); U.S. Embassies and/or other appropriate law enforcement officials, including ICE and CBP (specifically, NTC-P and NTC-C as appropriate); and appropriate members of the IC. For outbound ENCOUNTERS, or ENCOUNTERS involving subjects who have certain DEROGATORY INFORMATION, TSOU contacts (via phone and electronic notification) the appropriate counterterrorism element(s). Especially sensitive ENCOUNTERS often require coordination and situational updates with the White House, Northern Command (NORTHCOM), and FBI's Counterterrorism-Watch.

5.14 **TSC Actions.** TSC will update existing KNOWN or SUSPECTED TERRORIST records with new TERRORIST IDENTIFIERS and TERRORISM INFORMATION and will provide the broader counterterrorism analytic community with as much new information as possible stemming from an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST. TSC's primary methods for sharing TERRORISM INFORMATION with the broader counterterrorism analytic community will be through its EMA application and the use of Intelligence Information Reports (IIRs), as described further in Section V, *infra*. TSC will also coordinate with Fusion Centers on law enforcement and other ENCOUNTERS impacting their Area of Responsibility. This coordination will include a request for record enhancing information from the Fusion Center, which if received, will be added to the subject's KNOWN or SUSPECTED TERRORIST record.

5.14.1 Any new TERRORISM INFORMATION recorded in, or attached to an EMA record by TSC will be provided to NCTC via an automated ingest process.<sup>89</sup> Such daily ingests of EMA records update NCTC's TIDE to reflect the fact of the ENCOUNTER, any new identifiers used to confirm the KNOWN or SUSPECTED TERRORIST POSITIVE MATCHES, or those identified in an IIR. Once TIDE has been updated, an automated ingest from TIDE to TSDB is used to update the various TSDB subsets (e.g., No Fly or Selectee Lists). At this point, the process is complete and the watchlisting, screening and law

---

<sup>89</sup> An "automated ingest" is one where the contents of TSC's EMA records are incorporated into NCTC's TIDE database via a system-to-system transfer of information that identifies new or changed information. This process allows NCTC to spot KNOWN or SUSPECTED TERRORIST records that have been amended or updated. This process also accommodates the transfer of attached ENCOUNTER PACKAGES received from SCREENERS. In those instances, the ENCOUNTER PACKAGES appear as attachments to the KNOWN or SUSPECTED TERRORIST record. ENCOUNTER PACKAGE attachments must be moved to another system in order to give the broader counterterrorism community access to the TERRORISM INFORMATION. That process is described in Section V, *infra*.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

enforcement communities have the most current and thorough TERRORISM INFORMATION available about a KNOWN or SUSPECTED TERRORIST. Most—but not all—of that TERRORISM INFORMATION is available in a structured format as part of the KNOWN or SUSPECTED TERRORIST record (*e.g.*, discrete elements such as a date of birth, country of origin). The unstructured TERRORISM INFORMATION, while also in digitized format (*e.g.*, a computer disk, a scanned image of a business card, an encountering officer's report), is handled by NCTC.

- 5.15 **NCTC Actions.** NCTC will post to TIDE Online any digitized ENCOUNTER PACKAGE it receives from TSC or directly from a SCREENER. ENCOUNTER PACKAGES can be found under the subject's main page.

**V. ROLES AND RESPONSIBILITIES FOR UPDATING EXISTING KNOWN OR SUSPECTED TERRORIST RECORDS AND NOMINATING NEW KNOWN OR SUSPECTED TERRORISTS BASED ON INFORMATION FROM POSITIVE ENCOUNTERS**

- 5.16 This section describes the roles and responsibilities of the watchlisting, screening, and counterterrorism communities for exploitation and analysis of the TERRORISM INFORMATION lawfully collected and shared when there is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST. In this context the following definitions apply:

5.16.1 "INITIAL REVIEW" means a quick review of the ENCOUNTER PACKAGE to identify obvious, new TERRORIST IDENTIFIERS about the KNOWN or SUSPECTED TERRORIST.

5.16.2 "ADVANCED ANALYSIS" means a thorough review of the TERRORISM INFORMATION contained in an ENCOUNTER PACKAGE obtained as a result of the ENCOUNTER with the KNOWN or SUSPECTED TERRORIST. ADVANCED ANALYSIS includes the adding of TERRORIST IDENTIFIERS to existing KNOWN or SUSPECTED TERRORIST records and identifying new KNOWN or SUSPECTED TERRORISTS who should be nominated through the existing nomination process. In this context, ADVANCED ANALYSIS is being done on a tactical matter related to the specific KNOWN or SUSPECTED TERRORIST to identify information useful in "connecting the dots" between and among that KNOWN or SUSPECTED TERRORIST and other KNOWN or SUSPECTED TERRORISTS or potential KNOWN or SUSPECTED TERRORISTS. It is also when the need for foreign language translation services will be identified.

5.16.3 "TARGETED ANALYSIS" means further exploitation of a targeted set of ENCOUNTER PACKAGES and ADVANCED ANALYSIS products to assist in identifying TERRORIST trends and changes to methods, tactics, and practices. ENCOUNTERS for TARGETED ANALYSIS are selected using contemporaneous threat criteria and research in additional repositories. Contemporaneous threat criteria includes association with a priority terrorist group (*e.g.*, NIPF Tier I or II); ENCOUNTERS with KNOWN or SUSPECTED

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

TERRORISTS designated as No Fly or associated with violent activity; or at the request of any Department or Agency that identifies a need.

- 5.17 Results of INITIAL REVIEW, ADVANCED ANALYSIS, and TARGETED ANALYSIS efforts (collectively, "Exploitation") by Departments or Agencies will be reported to the watchlisting, screening and counterterrorism communities using standard templates when available.

**5.17.1 TSC Actions.**

5.17.1.1 **First Stage Review.** TSC actions with KNOWN or SUSPECTED TERRORIST ENCOUNTERS occur in two stages. The first stage occurs when the ENCOUNTERING AGENCY and TSC exchange TERRORIST IDENTIFIERS to determine whether the individual is watchlisted (*i.e.*, a POSITIVE MATCH to a TSDB record). TSC records any new TERRORIST IDENTIFIERS provided during this stage in TSC's EMA application.

5.17.1.2 **Second Stage Review.** The second stage occurs after TSC has confirmed there is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST. For each POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST, the TSC's Office of Intelligence (TSC/OI) will generate an IIR for dissemination to the counterterrorism community that provides a summary about the KNOWN or SUSPECTED TERRORIST ENCOUNTER (*e.g.*, basic facts about the ENCOUNTER such as date, time, and place). If available at the time the initial IIR is prepared, TSC/OI will conduct an INITIAL REVIEW of the ENCOUNTER PACKAGE and provide a thumbnail summary of the TERRORISM INFORMATION. For example, a summary might highlight the existence of a new KNOWN or SUSPECTED TERRORIST ("KNOWN or SUSPECTED TERRORIST was traveling with three other associates not previously identified in the car where the explosives were found in a hidden compartment") or the possibility that new TERRORIST IDENTIFIERS are available ("approximately 80 pages carried by the KNOWN or SUSPECTED TERRORIST were converted to electronic documents ranging from the KNOWN or SUSPECTED TERRORIST'S calendar/address book to bank account and credit card numbers").

5.17.2 **National Media Exploitation Center Actions.** Much of the TERRORISM INFORMATION generated by ENCOUNTERS from a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST is expected to be in a foreign language that may hinder prompt exploitation. The National Media Exploitation Center (NMEC) has the capability to translate foreign language information and the experience necessary to understand the efforts used to hide their activities. When TSC receives ENCOUNTER PACKAGES with information in a foreign language, or when NCTC receives them directly from an ENCOUNTERING AGENCY, TSC or NCTC will forward/notify NMEC that it has the action to translate the ENCOUNTER PACKAGE. Once the ENCOUNTER PACKAGE has been translated and returned to TSC and NCTC, the assigned roles and responsibility for exploitation will apply.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**5.17.3 FBI Actions.** The majority of the FBI's ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS occur in the United States. The FBI has ADVANCED ANALYSIS responsibility for ENCOUNTER PACKAGES on KNOWN or SUSPECTED TERRORISTS for whom the FBI has an open investigation, no matter where the individual is encountered. If the FBI does not have an open investigation on a KNOWN or SUSPECTED TERRORIST encountered in the United States, or if the KNOWN or SUSPECTED TERRORIST is a U.S. PERSON, then TSOU will send a lead directing the appropriate FBI field office to conduct an assessment of the individual and the ENCOUNTER circumstances to determine whether to open a preliminary or full investigation.<sup>90</sup> This assessment includes ADVANCED ANALYSIS packages when provided by ENCOUNTERING AGENCIES. If no investigation is opened, an IIR will be sent to the NOMINATING AGENCY and NCTC which will be used to enhance the TIDE record with additional FBI-derived information.

**5.17.4 DHS I&A Actions.** DHS I&A has ADVANCED ANALYSIS responsibility for ENCOUNTER PACKAGES where the KNOWN or SUSPECTED TERRORIST is denied entry, denied ESTA, denied boarding, or is subject to a no board recommendation at a foreign location, or identified through ICE's visa security processes.

**5.17.5 NCTC Actions.** On occasion, DOS, USAID, and foreign governments have ENCOUNTERS with KNOWN or SUSPECTED TERRORISTS, usually in the form of a record ENCOUNTER (*e.g.*, the KNOWN or SUSPECTED TERRORIST has submitted an application for a benefit like a visa or grant or information is provided to the United States by a foreign government). NCTC has ADVANCED ANALYSIS responsibility for ENCOUNTER PACKAGES in these instances.

**5.17.5.1** For TARGETED ANALYSIS, NCTC offers this capability for a select set of ENCOUNTER PACKAGES based on internal or interagency tasking. Since all ADVANCED ANALYSIS products created by FBI, DHS, or NCTC will be disseminated to the U.S. Government via an IIR, these materials are available to any organization seeking to further exploit specific ENCOUNTERS. NCTC will leverage these ADVANCED ANALYSIS products as part of its typical intelligence analytic process to highlight emerging threats, issues or concerns.

**5.17.6** A chart depicting the roles and responsibilities by Department or Agency may be found at the end of this Chapter.

## **VI. RESPONSIBILITY TO COORDINATE ANY ACTIONS CONTEMPLATED BASED ON INFORMATION FROM ENCOUNTERS WITH A KNOWN OR SUSPECTED TERRORIST**

<sup>90</sup> Under governing authorities, the FBI can conduct "assessments" for an authorized purpose, such as obtaining information about a threat to national security, without a particular factual predication. To open an investigation – whether a "preliminary" or "full" investigation – there must be a specific factual predication.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- 5.18 **Information Sharing MOU Requirements.** Departments and Agencies are reminded of their agreement to provide transparency between and among them with regard to their "activities to preempt, prevent, and disrupt TERRORIST attacks against U.S. PERSONS and interests."<sup>91</sup> As a practical matter, that type of transparency demands, to the greatest extent possible, prior coordination with affected Departments or Agencies before action within a Department or Agency's authorities is taken based on TERRORISM INFORMATION from a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST. For example, FBI, Central Intelligence Agency (CIA) or DOD, as lead counterterrorism Agencies in their respective domains, must be consulted prior to taking any action based on ENCOUNTERS with a person who is a POSITIVE MATCH with KNOWN or SUSPECTED TERRORIST. This guidance is subject to existing policies and coordination procedures when action against or pertaining to the KNOWN or SUSPECTED TERRORIST is contemplated.
- 5.19 **Requests for Withholding of Action.** In certain circumstances, law enforcement or the IC may request that a SCREENER not take action (e.g., not to refuse the visa, to allow individual to enter the United States, to not deny an individual to obtain an immigration benefit or access to the secure area of an airport) although action may be taken under the law. This request, to the extent practicable, shall be in writing, by a senior official, and include a statement of justification and risk mitigation. Departments and Agencies will establish mutually acceptable processes and procedures to implement a detailed plan.

## VII. EXAMPLES OF TERRORISM INFORMATION TYPICALLY AVAILABLE FROM ENCOUNTERS

- 5.20 The following examples of various types of ENCOUNTERS and the type of information typically generated from those ENCOUNTERS is offered to assist Departments and Agencies in understanding what additional or new information may become available as a result of following the guidance provided in this document.

- 5.20.1 **Ports of Entry.** Types of documents that could be included in the ENCOUNTER PACKAGE typically include:
1. Business cards
  2. Copies of passport and visa entries

---

<sup>91</sup> See Paragraph 3(b) of the *Information Sharing MOU* (Appendix 5): "Reciprocity and Transparency. All information collected by any entity relevant to the missions and responsibilities of any other covered entities should be shared, to the greatest extent possible, between and among all covered entities. Likewise, the parties agree that, to the greatest extent possible, there should be transparency between and among the covered entities with regard to their activities to preempt, prevent, and disrupt TERRORIST attacks against U.S. PERSONS and interests. Except as otherwise specified in this Agreement, or mandated by relevant Federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular covered entity plays as a provider or recipient of covered information. In other words, for example, international TERRORISM INFORMATION collected by the Border Patrol should be shared by DHS with the IC to the same extent foreign intelligence information on TERRORISM is shared by the IC with DHS."

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

3. Driver's license
4. Resumes
5. Conference literature
6. Correspondence not in possession of the U.S. Postal Service.
7. Letters of introduction
8. Checks, bank deposit slips
9. Calendar/schedule
10. Address book
11. Notepad entries
12. Mariner's certificates
13. Telephone data
14. Location and duration of previous travel stops on current or past travel itinerary

**5.20.2 Law Enforcement ENCOUNTERS.** Information collected from law enforcement ENCOUNTERS with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST can include any information that would be collected when a law enforcement officer speaks with a KNOWN or SUSPECTED TERRORIST. Typically information that could be included in the ENCOUNTER PACKAGE can include, but is not limited to:

1. Associates
2. Telephone numbers (home, business, cell, pager, or fax)
3. Other forms of identification
4. Physical descriptors
5. Family members
6. Occupation and work history
7. Travel plans or history
8. Vehicle information

**5.20.3 Visa Applications.** A typical DOS ENCOUNTER PACKAGE with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST will be a visa application for entry to the United States, which identifies basic information about the encountered KNOWN or SUSPECTED TERRORIST and the ENCOUNTER. Types of documents that could be included in the ENCOUNTER PACKAGE typically include:

1. Home and work address
2. Copies of passport and visa entries
3. National Identification Number (if applicable to the country)
4. Phone numbers (home, business, cell, pager, or fax)
5. Sponsorship information (when available, to include individual's name/Company/Government, address and contact information)
6. Family member names (e.g., spouse, parents, children)
7. Police Certificates (if applicable)
8. Biometrics (Photos and Fingerprint Identification Number (FIN))
9. Resumes (when applying for business visas)
10. Letters of introduction

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

11. Military related documents
12. Education
13. Prior travel
14. Occupation and work history
15. Financial information used to support visa application including bank statements, salary slips/letters, property records
16. Photos
17. Email addresses

**5.20.4 Applications or Petitions for Immigration Benefits.** USCIS may receive an application from an alien for immigration benefits or petitions. Depending on the completed form, USCIS may have information from the following non-exhaustive categories:

1. Residences domestic and foreign
2. Family Members (often extended family)
3. Occupation
4. Bank account information
5. Biometrics
6. Gender
7. Identity documents
8. Travel document information (and I-94)
9. Civil documents—POB, COC data
10. Employer/Prospective Employer
11. Religious Affiliations
12. Resumes
13. Educational Background
14. Past marriages or divorces
15. Biographical Information

**5.20.5 ENCOUNTERS by HSPD-6 Foreign Partners.** On some occasions, and based on the arrangement with and legal authorities of the particular foreign partner involved, an ENCOUNTER PACKAGE may include the KNOWN or SUSPECTED TERRORIST'S visa application to a foreign partner. One such student visa/permit application to a foreign partner could include information provided from the KNOWN or SUSPECTED TERRORIST in the following categories:

1. Name as shown in passport
2. Other names known by or ever known by
3. Name in ethnic script
4. Gender
5. Date of birth
6. Town/city of birth
7. Country of birth

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

8. Passport number, country, expiration date
9. Country of citizenship
10. Other citizenships held
11. Residential address and telephone number in home country
12. Local residential address and telephone number (if already in country)
13. Name and address for communication about this application
14. Name and address of friends, relatives, or contacts you have in the country (if applicable)
15. All periods of employment, including self-employment (to/from dates, name of employer, location, type of work/occupation/job title)
16. Financial information used to support visa application including bank statements, salary slips/letters, and property records
17. Length of planned stay in country
18. Questions concerning the person's character (e.g., whether the person has ever been convicted, charged, or under investigation for any offense(s) against the law in any country; ever deported, excluded or refused a visa by/removed from any country; and police certificates (as evidence of character) from home country or countries of citizenship and from all countries where the person has lived for five or more years since age 17)
19. Whether the application is for a student visa, a student permit, or a limited purpose visa
20. Whether the application is for a variation of conditions to work
21. Course of study and details of the course(s) enrolled
22. Arrangements for outward travel from host country
23. Name of legal guardian, other names legal guardian is known by, and relationship (e.g., mother, father, legal guardian)
24. Any national identity number or other unique identifier issued by a government
25. Any completed military service (e.g., from/to dates, rank, unit name or number, role)
26. Whether presently subject to military service obligation in any country
27. Any association with any intelligence agency or group, or law enforcement agency
28. Any association with any group or organization that has used or promoted violence to further their aims
29. Any involvement in war crimes, crimes against humanity, and/or human rights abuses
30. Payment method for application fee (e.g., bank check/draft, credit card, or personal check)

**VIII. OBTAINING ENCOUNTER INFORMATION THROUGH TSC'S DAILY ENCOUNTER REPORTS**

- 5.21 In addition to the aforementioned TSC/OI IIRs following an ENCOUNTER with a person who is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST, Agencies can obtain the Daily

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

Summary Report (DSR) to assist them in identifying ENCOUNTERS of interest to their organizational missions. DSRs will contain as much information as legally permissible. DSRs are available from the following locations:

5.21.1 On the Secret Internet Protocol Router Network (SIPRNET), [www.fbi.sgov.gov/](http://www.fbi.sgov.gov/), click on the "TSC Intel Daily Summary Reports" link on the right side.

5.21.2 On Law Enforcement Online (LEO) via [www.leo.gov](http://www.leo.gov)

5.21.3 On Regional Information Sharing Systems via [www.riss.net](http://www.riss.net)

5.21.4 On HS SLIC (for access contact state or local fusion center) or email: [\[REDACTED\]@hq.dhs.gov](mailto:[REDACTED]@hq.dhs.gov)

5.21.5 Two sources on FBINet:

5.21.5.1 TSC's homepage at <http://home.fbinet.fbi/nsb/tsc/Pages/Default.aspx>

5.21.5.2 Current Intelligence Report at <http://di.fbinet.fbi/ims/ciu/ciro/>

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

## Encounter Roles and Responsibilities

Entity	Type	Data Format	Recipients	Responsible Entity	Encounter Information and new Identifiers entered into IMA	Responsible Entity	Responsible Entity
DHS/CBP/NTC	Apprehension Detention APIS Query ASFA Pre-Flight Inspection Land Border Crossing Vessel Manifest Cargo Shipment Flight Manifests (Inbound and Outbound International)	Encounter Package	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Reviews Electronic Referral)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) DHS/ISA (is responsible for denied entries)	NCTC
DHS/ICE	Removal Investigation Extradition (in coordination with DOS and DOJ) DHS Recurrent Visiting DHS National Security Overlay Initiative	Encounter Package	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Reviews Electronic Referral)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) DHS/ISA (is responsible for denied entries)	NCTC
DHS/TSA	Secure Flight Credentialing (QIA) Pre-Flight Inspection Flight Manifests Other	Encounter Package	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Reviews Electronic Referral)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) DHS/ISA (is responsible for denied entries)	NCTC
DHS/USCIS	Applicant Petitioner Beneficiary	Application/ Previous Visa Applications	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS 4. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/CIS (Reviews Application)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) DHS/ISA (is responsible for denied entries)	NCTC
DHS/US Coast Guard	APIS Query Vessel Manifest Maritime Credentialing Vessel & Port Inspections Investigations Law Enforcement	Encounter Package	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) DHS/ISA (is responsible for denied entries)	NCTC
DHS/US Secret Service	Investigations Political and Special Events	Encounter Package	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DHS	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.)	NCTC
DOS	Visa Application	Current/Previous Applications	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DOS 4. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/DOS (Reviews Visa Application)	NCTC FBI	NCTC
	Visa Revocations	Current/Previous Applications	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DOS 4. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/DOS (Reviews Visa Application)	NCTC FBI	NCTC
	Passport Application	Current/Previous Applications	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. FBI 3. DOS 4. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Reviews Passport Application)	NCTC FBI	NCTC
USAID	Benefits	Application (When Available)	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. TSOU 3. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/USAID (Reviews Electronic Referral)	NCTC	NCTC
Foreign Government	Remote Query International	Foreign Government POC Referral/ Application (When Available)	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Reviews Electronic Referral)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) NCTC	NCTC
	Legacy & Other Countries	Foreign Government POC Referral/ Application (When Available)	1. NCTC (posts to NOL, NOL-J, NOL-S) 2. TSC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/DOS (Reviews Electronic Referral)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) NCTC	NCTC
Law Enforcement	National Instant Background Checks / Traffic Violation / Data Law Enforcement Investigation / Jail Related / Domestic Dispute / Arrest / Extradition	FBI CA/ITF forwards Biometrics, Police Report (When Available)	2. FBI 3. NCTC	1. TSOU-Operational Notification 2. TSC-01 (IR)-Community Notification	TSC/TSTOC (Via Telephone Call)	FBI (Open cases, USPER, or the RST is admitted/is in the U.S.) NCTC	NCTC

\* \* Section 6, *infra*, identifies categories of terrorism information from encounters with positively identified known or suspected terrorists that are of potential interest to researchers, other counterterrorism analysts, or the watchlisting community. Encountering entities should collect and share when it is within their legal authorities to retain and share terrorism information.

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION



**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**

- A. **ADVANCED ANALYSIS:** is a thorough review of the TERRORISM INFORMATION contained in an ENCOUNTER PACKAGE obtained as a result of the ENCOUNTER with the KNOWN or SUSPECTED TERRORIST. ADVANCED ANALYSIS includes the adding of TERRORIST IDENTIFIERS to existing KNOWN or SUSPECTED TERRORIST records and identifying new KNOWN or SUSPECTED TERRORISTS who should be nominated through the existing nomination process. In this context, ADVANCED ANALYSIS is being done on a tactical matter related to the specific KNOWN or SUSPECTED TERRORIST to identify information useful in "connecting the dots" between and among that KNOWN or SUSPECTED TERRORIST and other KNOWN or SUSPECTED TERRORISTS or potential KNOWN or SUSPECTED TERRORISTS. It is also when the need for foreign language translation services will be identified.
- B. **AGGREGATORS:** are those who receive and hold TERRORISM INFORMATION and certain other non-TERRORISM INFORMATION they are authorized to receive and retain.
- C. **DEROGATORY INFORMATION:** is intelligence or information that demonstrates the nature of an individual's or group's association with TERRORISM and/or TERRORIST ACTIVITIES.
- D. **ENCOUNTER:** is an event in which an individual is identified during a screening process to be a "POSITIVE MATCH," "POTENTIAL MATCH," or "INCONCLUSIVE MATCH," to an individual who has been designated in the TSDB as a KNOWN or SUSPECTED TERRORIST. An ENCOUNTER can be a face-to-face meeting with a KNOWN or SUSPECTED TERRORIST, electronic or a paper-based ENCOUNTER (e.g., the KNOWN or SUSPECTED TERRORIST has submitted an application for a benefit like a visa, ETSA grant, or information is provided to the United States by a foreign government, aircraft operator, or other private entity).
- E. **ENCOUNTERING AGENCY:** is a Department or Agency of the U.S. Government with TERRORIST screening or law enforcement responsibilities that comes into contact with a KNOWN or SUSPECTED TERRORIST (whether in a face-to-face situation or via an electronic or written submission such as an application for a benefit) that the TSC determines is a POSITIVE MATCH to a KNOWN or SUSPECTED TERRORIST.
- F. **ENCOUNTER PACKAGE:** is all information gathered during an ENCOUNTER with a KNOWN or SUSPECTED TERRORIST.
- G. **ENHANCEMENT:** is the addition of new TERRORIST IDENTIFIERS or DEROGATORY INFORMATION on a KNOWN or SUSPECTED TERRORIST.
- H. **FOREIGN FIGHTERS:** are nationals of one country who travel or attempt to travel to another country to participate in TERRORISM and/or TERRORIST ACTIVITIES.
- I. **FRAGMENTARY INFORMATION:** is information that suggests an individual may have a nexus to TERRORISM and/or TERRORIST ACTIVITIES but the information available to the NOMINATOR does not meet either or both the minimum identifying criteria that will facilitate identification of these individuals or the substantive DEROGATORY INFORMATION to meet the REASONABLE SUSPICION standard but does qualify as information that should be provided to NCTC pursuant to HSPD-6.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION**



## UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

- J. **INCONCLUSIVE MATCH:** is the final determination by TSC that limited information in the subject data set matches TSDB data in a TSDB record and no additional identifiers are available to verify the match.
- K. **INITIAL REVIEW:** is a quick primary review of the ENCOUNTER PACKAGE to identify obvious, new TERRORIST IDENTIFIERS about the KNOWN or SUSPECTED TERRORIST.
- L. **KNOWN TERRORIST:** is an individual whom the U.S. Government knows is engaged, has been engaged, or who intends to engage in TERRORISM and/or TERRORIST ACTIVITY, including an individual (a) who has been, charged, arrested, indicted, or convicted for a crime related to TERRORISM by U.S. Government or foreign government authorities; or (b) identified as a terrorist or member of a designated foreign terrorist organization pursuant to statute, Executive Order or international legal obligation pursuant to a United Nations Security Council Resolution.
- M. **LONE WOLF:** an individual motivated by one or more extremists ideologies, who operates alone and supports, or engages in acts of violence in furtherance of that ideology or ideologies that may involve direction, assistance, or influence from a larger terrorist organization of a foreign actor.
- N. **NOMINATOR or NOMINATING DEPARTMENT OR AGENCY:** is a Federal Department or Agency that has information to indicate that an individual meets the criteria for a KNOWN or SUSPECTED TERRORIST and nominates that individual to TIDE and the TSDB based on information that originated with that Department or Agency and/or a third Department or Agency.
- O. **OPERATIONALLY CAPABLE:** as described in Chapter 4, an individual is "OPERATIONALLY CAPABLE" if, based on credible intelligence, he or she, acting individually or in concert with others, reasonably appears to have the ability, knowledge, opportunity, and intent or is actively seeking the opportunity to engage in a violent act of TERRORISM consistent with 18 U.S.C. 2331 or 18 U.S.C. 2332b. For example, attempting to obtain an IED would indicate an individual is OPERATIONALLY CAPABLE of committing an act of TERRORISM. However, simply conducting internet research concerning IEDs would not be sufficient without additional activity. Depending on circumstances, and in combination with other facts, scouting potential targets or traveling for no legitimate purpose to places that have TERRORIST training grounds, regardless of whether the person is presently capable of using an IED, might also indicate an individual is OPERATIONALLY CAPABLE of committing an act of TERRORISM.
- P. **ORIGINATOR:** is the Department or Agency that has appropriate subject matter interest and classification authority and collects TERRORISM INFORMATION (*i.e.*, raw information) and disseminates it or TERRORIST IDENTIFIERS to other U.S. Government entities in an intelligence report (*i.e.*, finished intelligence) or other mechanism.
- Q. **PARTICULARIZED DEROGATORY INFORMATION:** is the type of information relied on to determine whether REASONABLE SUSPICION is met. This is information that demonstrates the nature of an individual's or group's association with TERRORISM and/or TERRORIST ACTIVITIES

UNCLASSIFIED//FOR OFFICIAL USE ONLY/SENSITIVE SECURITY INFORMATION

SECRET//NOFORN

---

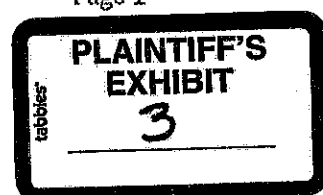


**Directorate of Terrorist Identities (DTI)  
Strategic Accomplishments 2013**

---

SECRET//NOFORN

Page 1



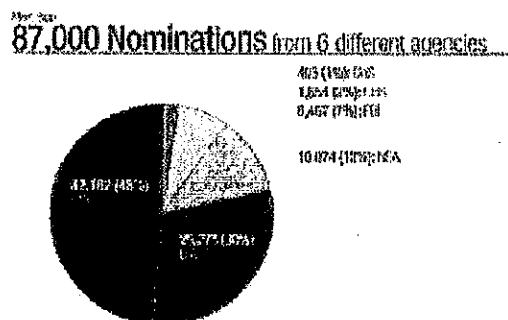
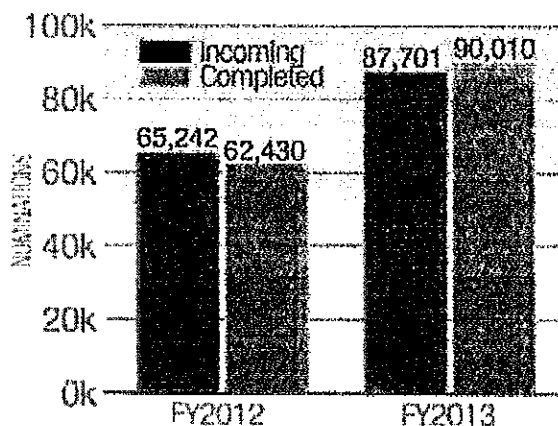
SECRET//NOFORN

**DTI Accomplishments Supporting NCTC Goal 1: Leadership**

(S//NF) **One Millionth TIDE Person Record:** On 28 June 2013, the Terrorist Identities Datamart Environment (TIDE) passed a milestone of one million persons in TIDE. While NCTC's Directorate of Terrorist Identities (DTI) seeks to create only as many person records as are necessary for our nation's counterterrorism mission, this number is a testament to DTI's hard work and dedication over the past 2.5 years. Since DTI stood up as an independent NCTC Directorate in December 2010, analysts have created more than 430,000 terrorism-related person records and deleted 50,000 subjects whose nexus to terrorism was refuted or did not meet current watchlisting criteria. In addition, DTI has added over 730,000 biometric files to TIDE. On a daily basis, DTI analysts process more than 250 nomination cables and 200 encounter reports, visa applications and other data sources to support the U.S. Government's (USG) screening and terrorism analysis missions.

(U//FOUO) **Processing Nominations Into TIDE:**

In 2013

**TIDE Nominations**

(S//NF) **Kingfisher Expanding its Role:** NCTC deployed the Kingfisher Expansion (KFE) visa support program on 15 June, 2013. KFE is a recently developed terrorist screening tool that correlates large datasets to help enhance existing terrorist identity information to support USG watchlisting/screening missions. The KFE tool reviews DoS visa applications for connections to terrorism information and then uses the knowledge to enhance existing records maintained in TIDE. KFE performs a near real-time check against TIDE for all worldwide visa applicants prior to Department of State (DoS) approval. KFE is processing nearly 40,000 applicants each day, has processed over 4.6 million visas since its "go-live" date in June, and is projected to save the DoS over \$50 million in security check fees.

SECRET//NOFORN

SECRET//NOFORN

**(S//NF) DTI Support to Boston Bombing Investigation:** In the wake of the Boston Marathon bombings, NCTC/DTI was deeply involved with all facets of the response. Immediately following the incident, DTI contributed to FBI deep dives, identified potential suspects, and delivered information to national leadership as well as coordinated with the FBI on biometric holdings in TIDE. Longer-term, DTI responded to the US Senate and House Congressional Intelligence Oversight Committees and prepared formal testimony that aided the Director of NCTC, Principal Deputy Director of NCTC, and Director of DTI for appearances on Capitol Hill. From this incident, DTI identified several lessons learned that were incorporated into the Directorate's policies and processes.

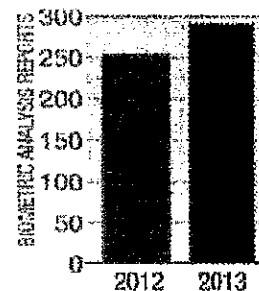
**(U//FOUO) Terrorist Identities Datamart Environment (TIDE) Classification Guide (CG):** Working with community partners, DTI finalized the first copy of the TIDE CG. This guide will serve as the official document for general classification guidance and classification policy controls and procedures for the dissemination and use of TIDE information, ensuring it will be adequately protected.

**(S//NF) Biometric Enhancement Scrub for Watchlisted US Persons:** Through a comprehensive review of TIDE holdings relevant to the Boston Marathon bombing, NCTC recognized the need to ensure that watchlisted US persons included available facial images and fingerprints. This project includes record by record research of each person in relevant Department of State and IC databases, as well as bulk data requests for information. The bulk requests were sent to our partners at FBI and DHS for any related biometric data, including driver's license images. When the project started there were 814 US Persons without any biometric information in TIDE, equating to less than 20% of the total watchlisted US persons. Upon completion of this project, NCTC has added 370 facial images and 249 fingerprints for 163 US persons.

**(S//NF) Mali and Chechnya/Dagestan Enhancement Scrubs:** In FY13, DTI completed a targeted scrub of TIDE subjects with connections to Mali or terrorist groups known to operate in Mali based on the recent conflict and ongoing threat to US and Western interests there. Separately, TIDE subjects with a nexus to Chechnya or Dagestan were reviewed in the wake of the Boston Marathon bombing.

- DTI analysts reviewed more than 1,700 TIDE records on subjects associated with these threats, resulting in some 3,500 enhancements to over 600 TIDE records.
- The scrub also resulted in watchlist status upgrades for 55 TIDE subjects.

**(S//NF) Biometric Analysis Reports:** The Biometric Analysis Branch (BAB) continues to provide support to a broad customer base through their unique skill of facial identification support. In 2013, BAB produced 291 Biometric Analysis Reports which provide facial identification support to customers from NCTC, DOD (AFOSI, SOCOM, PACOM), DOS, CIA, NMEC, DHS (CBP, NTC), FBI (TSC), DIA, NSA and NYPD.

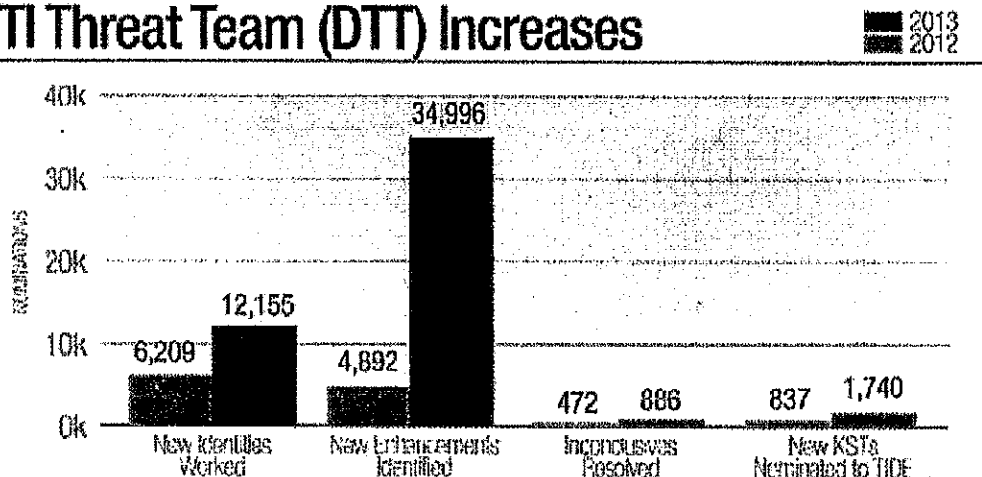


SECRET//NOFORN

Page 3

SECRET//NOFORN

(U//FOUO) DTI Threat Team (DTT/MTT):

**DTI Threat Team (DTT) Increases**

**(S//NF) Reduction of TIDE Enhancement Backlog:** This year, automation, policy modifications, and resource realignments helped reduce a historic backlog of Department of State Consular Consolidated Database (CCD) records consisting of visa information on KSTs that are already in TIDE and/or watchlisted in the TSDB. DTI had experienced a historical backlog that numbered in excess of 153,000 records. This number was reduced by 88% in FY13 to around 18,000 and that should be completely eliminated by Q1 2014. This reduction will allow for all newly identified KST TIDE records to be enhanced with CCD information within 48 hours of nomination.

**(S//NF) NCTC Meets HSPD-24 Requirements for Biometric Export:** In March 2013, in accordance with HSPD-24/NSPD-59, the full implementation of the biometric export occurred. This culminates a five year effort, which included significant changes such as moving from TIDE1 to TIDE2, in order to provide storing and matching capabilities for facial images, fingerprints and iris scans. As part of this effort, NCTC delivered biometric data for more than 127,000 known or suspected terrorists (KSTs) to the Terrorist Screening Center to date. Due to the hard work by NCTC, writ large, these KSTs will have their biometric data properly placed into the biometric screening systems. This means when one of these known or suspected terrorists attempts to enter the United States either by applying for a visa or through a DHS point of entry screening, regardless of falsified documentation, the subject will likely be denied entry.

**(S//NF) Growth for Non-Traditional Biometric Data:** DTI has continued to enhance several "non-traditional" biometric data fields in TIDE, for FY13 TIDE has shown the following growth: Handwriting (32%); Signatures (52%); Scars/marks/tattoos (70%); DNA strands (90%). Beginning collection on this data helps to ensure that when the biometric and forensic community is ready to actively screen this data, that NCTC will be readily able to provide the appropriate data on all known or suspected terrorists.

SECRET//NOFORN

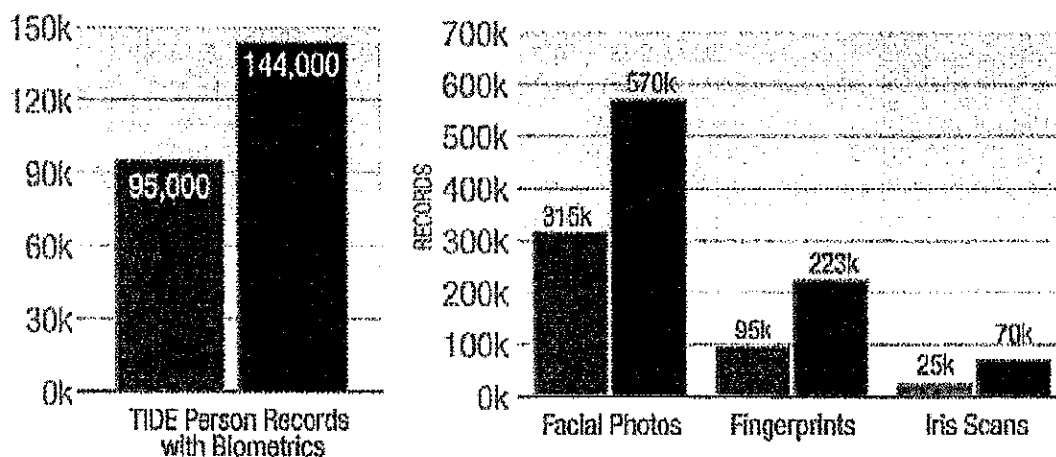
Page 4



SECRET//NOFORN

(S//NF) TIDE Records Enhanced with Biometrics data:

## Increased TIDE Biometric Holdings in 2013



(S//NF) **Biometric Data Sources:** DTI has seen a large increase of biometric data in 2013, both actively received from the nominating partners as well as proactively sought by the Identity Intelligence Group. The top five agency contributors of data are as follows: Department of Defense (60%), DHS (13%), CIA (12%), FBI (9%) and State Department (5%).

(S//NF) **FBI Platinum Project Support:** Since 17 June 2013, DTI reviewed 1,678 TIDE nomination cables in support of the FBI's Platinum Project. The Platinum Project was initiated by the TSC Nominations and Data Integrity Unit (NDIU) as a proactive means to identify FBI subjects of interest and US Persons who are nominated by Other Government Agencies (OGA) and are currently watchlisted in the TSDB. DTI conducted research in the FBI's Sentinel and Guardian databases to determine if the subjects identified in nomination cable traffic had an open or closed case or Guardian lead. This year, 1,142 Platinum leads were submitted to the FBI resulting in 42 new threat assessments, 5 preliminary investigations, one full field investigation, and four individuals being removed from the watchlist.

(U//FOUO) **Quality Assurance Requests:** More than 1,000 de-merge requests were reviewed to ensure that records which had incorrectly identified multiple subjects as one person, were appropriately divided into separate records. Conversely, over 6,500 person merges, nearly 13,000 location merges, and 11,200 merges of other entities was done, this removed duplicate data from TIDE and ensured the accuracy of these records.

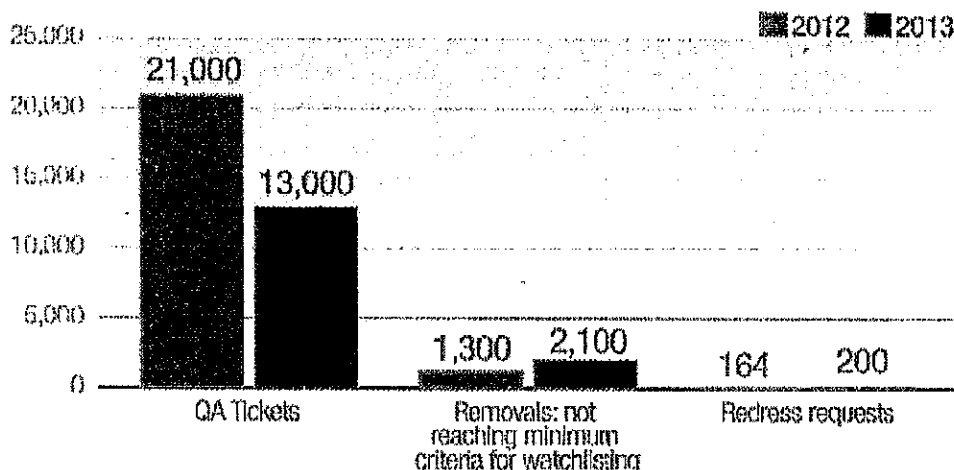
SECRET//NOFORN

Page 5

SECRET//NOFORN

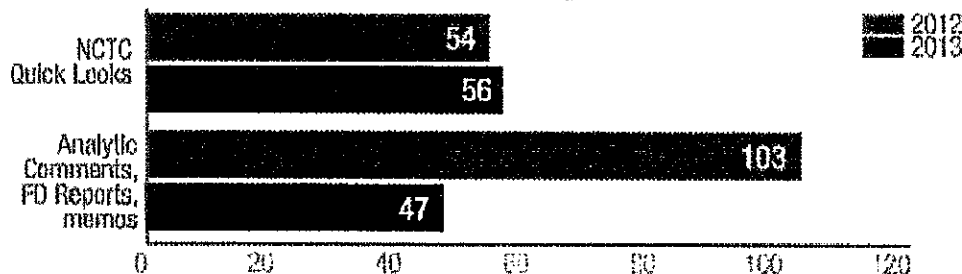
(U//FOUO) TSC Requested TIDE Quality Assurance Reviews:

More than

**15,300 TIDE Quality Assurance Reviews**

(U//FOUO) TIDE Quality Assurance Reviews: The Quality Assurance Branch (QAB) reviewed 6,500 legacy records as part of a proactive scrub of 60,000 single-source TIDE records where no update has occurred since January 2011. QAB reviewed records for 2,550 KSTs from visa waiver countries and 3,800 of the qualifying records that were created between 1994 and 1996. This work resulted in: 61 individuals removed from watchlisting (including 30 deletions from TIDE); three upgrades to TSA NOFLY; nine records merged with other entries; and 39 records with added biographic data. Additional enhancement work by the Identity Enhancement Team on 500 of the visa waiver records resulted in 10 watchlisting upgrades, and the addition of 47 first-time dates of birth, and 14 biometric files.

(U//FOUO) 2013 Analytic Products:

**Terrorism Identities Analysis Production**

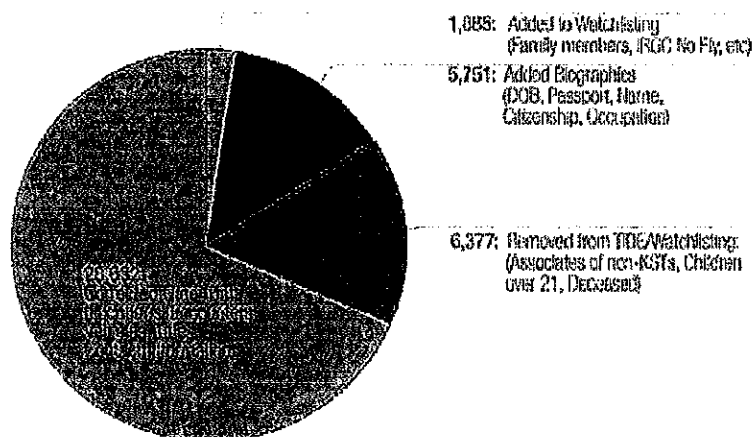
SECRET//NOFORN

Page 6

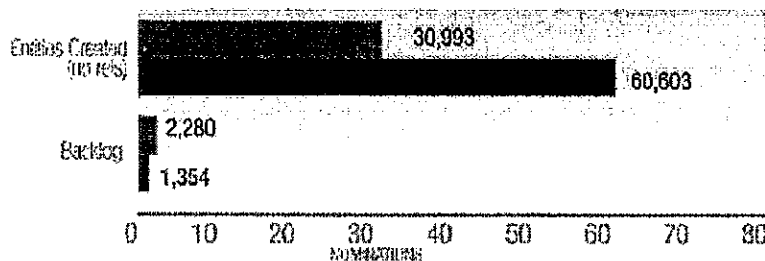
SECRET//NOFORN

**(S//NF) TIDE Quality Assurance Special Projects:**

More than

**41,800 Updates** from more than 21 different scrubs**(S//NF) Enhancements Using CBP Data:**

In 2013, more than

**6k CBP Encounter Packages Exploited****DTI Accomplishments supporting NCTC Goal 2: Partnership****Internal to NCTC:**

**(S//NF) Threat Case Management and Syrian Foreign Fighters:** In 2013, DTI created and maintains 12 threat cases, which link all known actors--and their biographic and biometric identifiers--to a particular threat stream, providing analysts across the community one centralized resource. The cases were collaborative efforts with NCTC/DI and DSOP, DHS/I&A, CBP, and TSA.

SECRET//NOFORN

Page 7

---

SECRET//NOFORN

---

The Syria Foreign Fighter Threat Case in TIDE provides the IC's common record for the activities of more than 3,200 KSTs associated with Syria. This case contains a total of 3,258 individuals, to include 715 Europeans and Canadians and 41 US Persons, 37 of which are watchlisted in TSDB.

External to NCTC:

**(S//NF) Chicago Marathon supported by DTI IIG and AEG TIDE Analysts alongside FBI:** Based on the lessons learned from the Boston Marathon, DTI analysts in AEG and IIG worked alongside the FBI and the NCTC Midwestern Representative to support the Chicago Marathon. Analysts performed deep dives in Tide for biometrics, and located all of the entries that had no photo or fingerprints. Analysts also pulled all of the records in TIDE of people who held a drivers license in Illinois, Indiana, and Wisconsin. Doing their due diligence with those TIDE lists, analysts ensured no one warranted further scrutiny by the FBI before the race.

**(S//NF) Biometric Support to NCDC:** In FY13, DTI began assisting the National Collaboration Development Center (NCDC) with their Targeting Collaboration Course (TCC). The TCC is an interactive scenario-based training in which students learn to enhance existing source identification skills by providing tactical analysis intended to spur an operational action against a human target.

**(U//FOUO) Driver's License Initiative:** To fulfill the biometric enhancement mission within DTI's Identity Intelligence Group (IIG), the Biometric Analysis Branch (BAB) began an outreach/partnership effort with the larger law enforcement community to collect facial images associated with driver's license data. With support from FBI partners and NCTC's Domestic Representatives, this enhancement mission took on significant growth in FY13. BAB now coordinates directly with the following states: Arizona, Texas, New York, Maryland, Delaware, Washington DC, Florida, California, Virginia, Oregon, Massachusetts, Nevada, Georgia, Colorado, Washington, and Rhode Island. This effort has resulted in 2,400 Driver's License facial images added to TIDE in FY13.

**(S//NF) International Travel Data (ITD):** DTI identified information gaps between TIDE and CIA's ITD and worked with CIA to add the missing data to TIDE from clandestinely collected travel data. This effort resulted in the inclusion of 892 fingerprint files and an additional 1268 data points added to TIDE. DTI used the data to enhance a total of 892 identities in TIDE.

**(U//FOUO) CMO Outreach Initiative:** To increase the biometric and biographic information on KSTs detained worldwide, DTI began working with the CIA's Collection Management Officers. As a result, over 150 requests have been sent to the field and nine new national HUMINT collection requirements have been written. Additionally, DTI is now sending collection requirements directly to the field using the CIA Information Needs Management database (CINEMA). This will allow DTI to obtain information that has not been collected and use it to enhance TIDE.

---

SECRET//NOFORN

Page 8

---

SECRET//NOFORN

---

(U//FOUO) **DTI Outreach Efforts:** DTI officers, together with representatives from the Terrorist Screening Center's (TSC) training team, traveled to FBI Miami and FBI Los Angeles, visiting Field Offices and fusion centers to educate analysts and agents about DTI, TSC, TIDE, and the watchlisting business process to aid in their role of reviewing case information and Guardian leads, and participation in the Encounter process. 2013 is the first year that DTI and TSC have partnered to provide outreach and training outside of the metro DC area.

(U//FOUO) **Training Expanded for External Partners:** DTI officers traveled to Glynco, GA to provide a brief to approximately 50 Counterterrorism Division instructors and leads at the Federal Law Enforcement Training Center (FLETC). The goal was to establish a partnership with FLETC and to educate the instructors about DTI, TIDE, and the watchlisting business process. In the WMA, DTI has also expanded its training offerings, holding a quarterly training session in the LX auditorium for all IC members. In FY13, DTI provided advanced TIDE training to 95 analysts representing nine partner agencies (TSC, TSA, NSA, DoS, DHS, FBI, CPB, US Army Special Forces, and Bureau of Diplomatic Security).

(S//NF) **Biometric Training Program Offered to Additional Partners:** DTI now offers a half-day Biometrics Training Program once a month that is open to all IC partners holding a TS/SCI clearance. The course provides a basic familiarization of classified and unclassified biometrics repositories; an overview of the watchlisting process as it pertains to biometrics and Identity Intelligence; and an introduction to targeted biometrics research at NCTC.

(U//FOUO) **DTI, TIDE and Watchlisting Review:** This review brought together experienced members of the watchlisting community to take a genuine look at how the community is doing. Participants were asked to put the views of their home agencies aside and take an objective look at the watchlisting process, TIDE, and DTI's support of TIDE and the watchlisting process. The exercise culminated in an assessment paper providing five key findings, seven recommendations for improvements, and acknowledging those areas that excel.

(S//NF) **CIA – Hydra:** DTI has partnered with CIA to enhance select populations in TIDE with clandestinely acquired foreign government information from CIA's Hydra program. In this multi-phased project, DTI provides CIA with TIDE data and it is correlated with Hydra information to uncover additional Terrorism Information (TI) on KSTs that is then used to conduct Quality Assurance reviews on existing TIDE records. As proof of concept, DTI provided CIA a list of 555 Pakistan based subjects identified as KSTs in TIDE. The Hydra program vetted these names against Pakistani Passports and provided TIDE record enhancement information (biographic and biometric identifiers) back to DTI. The next step will be to provide CIA with a list of TIDE subjects with National ID Numbers (~1,700) for vetting on dates of birth. Future initiatives will include additional targeted countries, as well as a targeted effort to locate first-time DOBs for subjects with Passports and National ID Numbers.

(U//FOUO) **Watchlisting Guidance Review IPC:** In 2013 the Watchlisting Guidance Review IPC completed a major, multi-year effort to review and update the July 2010

---

SECRET//NOFORN

Page 9



SECRET//NOFORN

Watchlisting Guidance. DTI participated in multiple detailed reviews providing comments and inputs and provided suggestions for improving the Guidance. The effort culminated in an approval by the Deputies Committee (DC) in March 2013.

(U//FOUO) **INTERPOL Information-Sharing Agreement:** INTERPOL Red Notices contain derogatory information, biographics, and biometrics which can serve to both create new TIDE records and enhance currently existing records. Through coordinated efforts, processes were developed whereby the FBI's National JTTF served to nominate subjects of Red Notices to TIDE for watchlisting and EAB is enhancing existing TIDE records with active Red Notices.

(S//NF) **Foreign Collected Terrorist Biometrics:** In 2012, the Biometric Analysis Branch partnered with FBI's Global Initiatives Unit to nominate biometric data captured on terrorists from foreign partners into TIDE. This process has continued to evolve and grow. In FY13, this process has enhanced over 1,000 terrorist records enabling effective biometric screening.

(S//NF) **National Media Exploitation Center (NMEC):** The Biometric Analysis Branch continued to support a DTI liaison within NMEC which proved beneficial to both organizations. The arrangement enables NCTC to obtain additional data fusion points by accessing and exploiting NMEC data holdings and, in return, DTI provides NMEC with a classified biometric search capability against TIDE through automated and manual facial identification support. To date BAB has enhanced 33 TIDE records and provided over 7,000 search results to NMEC. From this effort, in December 2012, the Encounter Analysis Branch established a CBP Encounter Package foreign document translation process with the National Media Exploitation Center and has completed 119 requests for translation and addendums to TIDE.

### **DTI Accomplishments supporting NCTC Goal 3: Workforce**

(U//FOUO) **DTI Internal Training:** Standard DTI Internal Training: In 2013, DTI provided training for a total of 124 new hires, a 100% increase over 2012. Over 80 of these new hires were trained during a two month period during the contract transition, an 800% increase over the previous two months. The training team was able to make considerable adjustments to accommodate this extremely high influx of personnel. In addition, DTI has developed and implemented a refresher course that provides incumbent analysts the opportunity to reinforce the fundamentals of TIDE production. The course highlights general policy and process updates of which analysts may not be aware given the different focus areas of the various branches within DTI. Finally, DTI developed a familiarization course for those in DTI who are interested in gaining a perspective on DTI operations. Topics include overviews of external IC policies, watchlisting, Kingfisher, TIDE, Biometrics, and DTI overview. A pilot and a full session ran in 2013.

(U//FOUO) **Mock CAB:** DTI's Professional Development Working Group sponsored mock Career Advisory Boards (CABs), which were designed to provide employees insight to the

SECRET//NOFORN

Page 10

SECRET//NOFORN

---

documentation and process involved in CAB decisions. Volunteer CAB panelists reviewed fictitious persons' PERs and bios and drafted Employee Assessment Forms for the "employee" they represented on the panel. ADD/DTI and DTI/COS acted as panel chairs to guide the process and facilitated an open discussion after the panels completed their employee evaluations. Participants gleaned insight into the importance and complexities of documentation and the process.

(U//FOUO) **Expansion of Identity Intelligence (I2) Training Module:** The training is taught once a month and has been well received across the community. This external course consists of a half day version of the DTI's Biometric Training Program. In addition, as an effort to ensure that every analyst within DTI has a basic understanding of biometric data and workflows, a shortened version of the training was incorporated into the MIO Training and Outreach Team portfolio. The additional DTI course consists of a one hour block which has been incorporated into both the DTI New Hire Training as well as the DTI Manager Training as of June 2013.

### **DTI Accomplishments supporting NCTC Goal 4: Process**

(U//FOUO) **DTI Policy Response Team:** DTI implemented a key process for addressing, coordinating, and responding to critical issues/actions such as the responses to the Boston Marathon bombing, Congressional questions for the record, White House requests for information and policy coordination DNI taskings, and NCTC directed actions. The team ensures taskings are researched before being sent out across the Directorate, coordinated appropriately within DTI, and that responses are consolidated and accurate. Since January the team has successfully researched and responded to over 110 actions.

(U//FOUO) **Governance Structure:** DTI established an internal governance structure to encourage the exploration of new ideas, prioritization of activities, and enable informed decision making. The two new groups, the Group Chief's Forum and the Futures Forum provide a process for ideas and workflows to be vetted and pushed up for decision.

(U//FOUO) **Applied Correlation to TIDE (ACT):** The ACT initiative enables DTI analysts to correlate TIDE data against various Intelligence Community and Law Enforcement databases. Using the new "correlate" function in TIDE, analysts are able to quickly conduct a search across several databases to determine if there is any existing data that can be used to enhance a TIDE record. This functionality is currently being piloted within the QA and IIG teams to determine future uses.

(U//FOUO) **Facilitation of Strategic Planning Across DTI:** Starting in June 2013, DTI began executing & tracking progress on 33 initiatives in the current DTI strategic plan (published in Jan 13) while also supporting 9 DTI-assigned initiatives in the NCTC strategic plan (published Feb 13). Efforts on both strategic plans provide a venue to focus Directorate activities and facilitate strategic planning.

SECRET//NOFORN

Page 11

---

SECRET//NOFORN

---

(U//FOUO) **Development of Metrics to Minimize Individual Requirements to Track Work Completion:** DTI developed a monthly TIDE-based metrics template in May 2013 and began [retroactively] tracking several datasets effective 1 Jan 2013. Information collected includes data on nominations, nomination backlog, special projects/bulk ingest, new entities created, encounters, and QA audits.

### **DTI Accomplishments supporting NCTC Goal 5: Technology**

(U//FOUO) **Standard Nomination Tool:** DTI, along with Watchlisting Community partners, upgraded the standard nomination tool used to send data for entry into TIDE. Significant improvements were made to the user interface to streamline the process of submitting data and the inclusion of the TIDE Restricted capability provided nominating agencies the ability to ensure that data too sensitive for export to unclassified systems could be appropriately marked and handled by TIDE. This allows nominating agencies to provide more data than previously disseminated as appropriate controls are now in place to ensure the sensitivity of the data is accounted for.

(S) **Bulk Ingest capability:** DTI developed an internal self-service program to ingest large datasets for automated exploitation and enhancement of TIDE records. The self-service capability allows DTI to quickly ingest large datasets into TIDE in a flexible environment where those providing the technical support are fully trained on DTI's policies and work closely with those who will process the data. The result is fewer policy errors and the ability to quickly make modifications and set priorities based on DTI's needs. The program's efficiency has enabled DTI to ingest multiple datasets in the time that the previous process would have taken to prioritize the datasets.

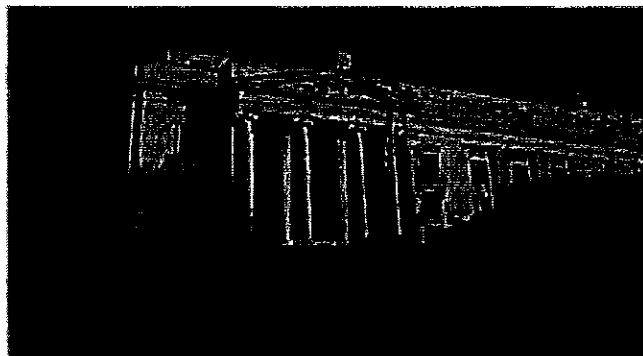
(U//FOUO) **Database Development** IIG's Data Exploitation Team developed a database which has created multiple efficiencies for internal processes. The database allows for automated tracking, metrics reporting, increased accuracy in de-duplication, and allows for tracking and identification of KSTs for further research. The database also allows for tracking of FISA classified cables. This database has saved at least 10 hours of work per week and has streamlined processes for RFIs, metrics, and identity management. Based on this success, this database has been duplicated for other internal DTI sections.

(S//NF) **EFT of CBP Packages to TIDE:** After 2-plus years of development, the early February 2013 approval of the *Interconnection Security Agreement* between CBP and NCTC resulted in the successful electronic file transfer of CBP Encounter Packages to TIDE. Previously, the Encounter Packages were retrieved from CBP via a Compact Disc. Since the 7 March 2013 start up, more than 5,378 Encounter Packages have been received and processed into TIDE by EAB.

---

SECRET//NOFORN

Page 12



# **AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF TERRORIST WATCHLIST NOMINATIONS**

U.S. Department of Justice  
Office of the Inspector General  
Audit Division

Audit Report 14-16  
March 2014

**REDACTED – FOR PUBLIC RELEASE**







# **AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF TERRORIST WATCHLIST NOMINATIONS**

## **EXECUTIVE SUMMARY<sup>1</sup>**

The Terrorist Screening Center (TSC) was created to consolidate the U.S. government's approach to terrorism screening and to develop and maintain a database of information about known or suspected terrorists, known as the Terrorist Screening Database (TSDB) or terrorist watchlist. The TSC is administered by the Federal Bureau of Investigation (FBI) with support from the National Counterterrorism Center (NCTC), the Intelligence Community, and law enforcement agencies.

On Christmas Day 2009, a Nigerian national, often referred to publicly as "the Underwear Bomber," attempted to detonate an explosive device onboard a flight from Amsterdam to Detroit.<sup>2</sup> Although the perpetrator of this failed attack was known to the U.S. government, he was not on the consolidated terrorist watchlist. As a result, the Watchlist Community took a series of actions to address immediate threats and improve the watchlist process. One objective of this OIG audit was to review the FBI's actions and evaluate the impact on the FBI's watchlisting system of this failed terrorist attack.

The OIG has performed five previous audits of watchlist-related activities and has made numerous recommendations to improve the watchlist. In addition to reviewing the impact of the December 25, 2009, failed terrorist attack, this audit also assessed the effectiveness of FBI initiatives, implemented between 2009 and 2012, that were intended to ensure the accuracy, timeliness, and completeness of the FBI's watchlisting practices, including watchlist nominations and removals.

### **Events Related to Terrorism Attempt on December 25, 2009**

Following the failed terrorist attack on December 25, 2009, the TSC was directed to make a series of temporary modifications to the watchlist status of several groups of individuals. These modifications were directed by an interagency process that involved high-ranking government officials in the Executive Branch and the White House. The changes reflected emerging threat information and were not covered by the then-existing watchlist policy and procedures. Overall, we found that the TSC responded commendably to the attempted terrorist attack and worked diligently to overcome these policy weaknesses, as well as the associated technical and procedural problems. However, we also determined that the

---

<sup>1</sup> The full version of this report contains classified and other information that if released publicly could compromise national security interests and the FBI's and TSC's operations. To create this public version of the report, the Office of the Inspector General redacted (blacked out) these portions of the report.

<sup>2</sup> The perpetrator ultimately entered a guilty plea and currently is serving a life sentence in federal prison.

modification requests were not communicated and documented effectively. In addition, as a result of the policy and procedural issues, the TSC was unable to readily identify individuals who met the threat-based criteria, or to easily generate a listing of all of the watchlist records that were modified in response to the directions provided subsequent to the incident. As a result, the TSC relied on largely manual processes to track the watchlist modifications and related in-depth or "deep dive" reviews related to the upgrades. In July 2010, the TSC and the Watchlist Community developed new policies and procedures to cover a similar event in the future.<sup>3</sup> Adhering to these policies and procedures should help to ensure that future threat-based watchlist modifications are communicated more effectively and coordinated more efficiently.

### **FBI Processing of Watchlist Nominations and Removals**

In general, individuals who are subjects of ongoing FBI counterterrorism investigations are nominated for inclusion on the watchlist. FBI policy also allows for the nomination of an individual for whom the FBI does not have an open terrorism investigation, referred to as non-investigative subjects.

During our previous audits of the FBI's watchlist processes, we found that the FBI failed to nominate to the watchlist subjects of terrorism investigations, failed to remove from the watchlist subjects of closed terrorism investigations, and was not timely in processing nominations to the watchlist.<sup>4</sup> In response to our reports, the FBI revised its watchlist policy, reorganized the operational unit responsible for processing watchlist nominations, implemented timeliness standards for the submission and processing of watchlist actions, and established a team to assess the FBI's performance against the new criteria. Further, the FBI implemented a new automated process for submitting and processing watchlist nominations and removals.

#### *Watchlist Nominations*

Generally, we found that the improvements implemented by the FBI as a result of our previous audits have helped to ensure that the watchlist is more complete, accurate, and current. For example, in our May 2009 audit we found that 15 percent of the subjects of FBI terrorism cases reviewed were not nominated to the watchlist. In our current review of 115 subjects of terrorism investigations opened during the first quarter of fiscal year (FY) 2011, we did not identify any subjects who were not nominated to the watchlist as required by FBI policy.

---

<sup>3</sup> Members of the Watchlist Community include the Office of the Director of National Intelligence, Central Intelligence Agency, National Geospatial Intelligence Agency, National Security Agency, National Reconnaissance Office, and the Departments of Justice, Defense, State, Treasury, Homeland Security, and Energy.

<sup>4</sup> The Department of Justice Office of the Inspector General has conducted five previous audits of the TSC, DOJ's watchlist nomination processes, and the FBI's watchlist practices. Additional details on these audits are provided in Appendix III.

However, we found that the FBI's December 2009 and December 2010 watchlist policies provided case agents with guidance about nominations to the watchlist that was inconsistent with the Watchlist Community's July 2010 Watchlist Guidance, and that the FBI policy unduly restricted the FBI's nominations to the watchlist. For example, the FBI's watchlist policy did not require the nomination of individuals for whom [REDACTED] were not known. However, the Watchlist Community's Guidance requires nominating agencies to share with NCTC and the TSC all terrorism-related information, including instances in which [REDACTED] is known. As a result, FBI case agents were not submitting certain nominations where [REDACTED] were not known. When we made this concern known to the FBI during the course of this audit, the FBI revised its watchlisting nomination guidelines in March 2012 to conform with the minimum identifying criteria set forth in the July 2010 Watchlisting Guidance. However, we believe the policy still provides FBI personnel with inconsistent directions that could cause terrorism information to not be available to the Watchlist Community.

Further, we found that during the course of an investigation, the case agent may obtain additional biographical information to meet the FBI's standard for nomination to the watchlist. However, an FBI official said that once the case agent obtains sufficient biographical information, the case agent should, but may forget to submit the appropriate paperwork to have the individual watchlisted. The FBI reported that its supervisors are required to conduct regular case file reviews with case agents to help ensure the subjects are appropriately watchlisted. However, despite these supervisory reviews, the subjects we identified for whom additional information was obtained during the investigation, were still not nominated to the watchlist while the case was open. In such instances, information about known or suspected terrorists would not be available to the Watchlist Community for analysis and possible watchlisting.

#### *Watchlist Removals*

We also found that subjects of closed terrorism investigations were removed from the watchlist when the case was closed. In our previous audit, we found that 8 percent of the subjects of the cases we reviewed were not removed from the watchlist when the case was closed. In our current audit, we found that the FBI removed from the watchlist subjects of cases closed in four field divisions during the first quarter of FY 2011.

#### *Watchlist Nomination and Removal Efficiency*

We also found that the FBI field divisions have improved their compliance with timeliness standards for the submission of watchlist nominations and removals to FBI headquarters. Nevertheless, we found that the FBI's time requirements for the submission of watchlist actions could be strengthened. Under the FBI's guidelines, up to 17 business days could elapse between the date a case agent receives supervisory approval to open a terrorism case and the date the subject is



nominated to the watchlist.<sup>5</sup> Based on our analysis of FBI watchlist data, we believe that the timeliness guidelines for the submission of watchlist actions by FBI field divisions could be reduced.

Moreover, we found that the FBI's headquarters unit that processes watchlist actions had redundant and inefficient processes that hampered its ability to process watchlist actions in a more timely fashion. During the course of our audit, the FBI developed and implemented new policies and procedures that we believe will help it to process watchlist actions more efficiently. Following the reorganization of the TSC and the headquarters unit responsible for processing FBI watchlist actions, we recommend that the FBI further review its policies and processes to determine the most effective and efficient methods, including technological improvements, to ensure that subjects are reliably nominated to the watchlist as expeditiously as possible.

### **FBI Watchlisting of Individuals Not Under Investigation**

During our previous audits, we identified weaknesses in the FBI's handling of watchlist records related to individuals who are not under investigation by the FBI, referred to as non-investigative subjects. The FBI issued a new policy that more clearly defined its processes for including on the watchlist such individuals for whom the FBI does not have an open investigation. In this audit, we found that the FBI used multiple processes to submit requests for watchlisting non-investigative subjects, and, the FBI was not timely in submitting watchlist nomination and removal packages for individuals not under investigation by the FBI. Most noteworthy is that during our review of a sample of non-investigative subject nominations, we identified four subjects of closed full investigations who had not been previously nominated to the watchlist. Although the case agent indicated that these subjects were eligible for inclusion on the Transportation Security Administration's (TSA) No Fly List, it took the FBI a median of 44 business days to submit the watchlist nomination package and nominate these subjects to the No Fly List.<sup>6</sup> Moreover, in cases where the FBI team determined that non-investigative subjects should be removed from the watchlist, it took the FBI a median of 78 days to remove the subjects from the watchlist. Finally, we found that the FBI had not maintained adequate records to readily provide an accounting of the time it took to process non-investigative subject nominations and removals or to document processing delays.

As a result of this review, the FBI implemented policies and procedures to help to ensure that its processing of non-investigative subject watchlist nominations is more complete, consistent, accurate, and timely. We believe that these improvements are a positive step forward. However, we identified continued

---

<sup>5</sup> The FBI also has an expedited nomination process, which is used when there is an imminent threat.

<sup>6</sup> The TSA No Fly List includes names of individuals who are to be denied transport on commercial flights because they are deemed a threat to civil aviation, U.S. facilities, or U.S. vessels.

weaknesses in the database used by the FBI to submit, monitor, and track non-investigative subject nominations.

Our report contains 12 recommendations to assist the FBI in strengthening its watchlist-related operations and practices. These recommendations include requiring the TSC to better document its actions during national security events, clarifying FBI information sharing policies to ensure the FBI's internal policies are consistent with those of the Watchlist Community, and improving the efficiency of the FBI's watchlist nomination process for investigative and non-investigative subjects.





# AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF TERRORIST WATCHLIST NOMINATIONS

## TABLE OF CONTENTS

INTRODUCTION .....	1
Failed Terrorist Attack of December 25, 2009 .....	2
Overview of the Watchlist Process .....	2
Overview of Internal FBI Watchlist Processes .....	7
Previous OIG Reviews .....	11
OIG Audit Approach .....	12
FINDINGS AND RECOMMENDATIONS .....	14
I.    TSC ACTIONS FOLLOWING THE FAILED TERRORIST ATTACK OF DECEMBER 25, 2009 .....	14
TSC Actions Following the Terrorist Attack .....	14
In-Depth Record Reviews ("Deep Dives") .....	23
TSC Documentation Supporting Watchlist Modification .....	26
TSC Managerial Continuity and Significant National Security Events .....	29
Review of the U.S. Watchlisting System .....	30
Conclusion .....	30
Recommendations .....	31
II.   FBI WATCHLIST NOMINATIONS AND REMOVALS .....	33
Background .....	33
Recent FBI Watchlist Initiatives .....	34
FBI Watchlist Nominations .....	37
Watchlist Removal Policies .....	52
OIG Analysis of FBI Watchlist Removal Actions .....	54
Conclusion .....	61
Recommendations .....	63
III.  NON-INVESTIGATIVE SUBJECTS .....	65
Overview of the Non-Investigative Subject Watchlist Process .....	65
OIG Review of Non-Investigative Subject Watchlist Records .....	68
Conclusion .....	77
Recommendations .....	78
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS .....	79

STATEMENT ON INTERNAL CONTROLS .....	80
APPENDIX I: AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY .....	81
APPENDIX II: DOWNSTREAM SCREENING DATABASES .....	85
APPENDIX III: SUMMARY OF OFFICE OF THE INSPECTOR GENERAL AUDIT REPORTS.....	87
APPENDIX IV: WATCHLIST STATUS MODIFICATION INITIATIVES AND RELATED DEEP DIVE REVIEWS .....	91
APPENDIX V: FEDERAL BUREAU OF INVESTIGATION'S RESPONSE TO THE DRAFT REPORT .....	92
APPENDIX VI: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT .....	96

## **AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF TERRORIST WATCHLIST NOMINATIONS**

### **INTRODUCTION**

Following the terrorist attacks on September 11, 2001, the Terrorist Screening Center (TSC) was created to consolidate the U.S. government's approach to terrorism screening and to develop and maintain a database of information about known or suspected terrorists.<sup>7</sup> The consolidated watchlist is known as the Terrorist Screening Database (TSDB). The watchlist is utilized to provide information to downstream screening databases, including the No Fly List.

The TSC is a multi-agency organization administered by the Federal Bureau of Investigation (FBI) with support from the Office of the Director of National Intelligence's National Counterterrorism Center (NCTC), the Intelligence Community, and law enforcement agencies.<sup>8</sup> The NCTC is the government's main repository of information regarding international terrorism and counterterrorism, and it stores the data it collects on known or suspected terrorists in a database known as the Terrorist Identities Datamart Environment (TIDE). According to the TSC Memorandum of Understanding, which governs the structure and operations of the TSC, NCTC's TIDE database does not include purely domestic terrorism information.

The watchlist process serves as a critical tool in the U.S. government's efforts to combat terrorism by helping intelligence agencies, law enforcement officials, and screening personnel identify known and suspected terrorists and by providing direction on how to respond during an encounter with these individuals.<sup>9</sup> The watchlist is continually updated with new terrorist identities and new or revised biographical information gathered by U.S. intelligence and law enforcement

---

<sup>7</sup> On September 16, 2003, the President issued Homeland Security Presidential Directive 6 (HSPD-6), which directed the Attorney General to establish an organization to consolidate the government's approach to terrorism screening and provide for the appropriate use of terrorism information in screening processes. As a result, the Attorney General created a new organization, the TSC. The TSC created the consolidated terrorist watchlist. In addition, HSPD-6 required all federal law enforcement and intelligence agencies with terrorism information to share such information for purposes related to the watchlist.

<sup>8</sup> Section 1021 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) amended the National Security Act of 1947 to codify the creation of NCTC to serve as the primary organization in the U.S. government for analyzing and integrating all intelligence information possessed or acquired by the U.S. government pertaining to terrorism and counterterrorism. NCTC is a component of the Office of the Director of National Intelligence and was formerly known as the Terrorist Threat Integration Center.

<sup>9</sup> An "encounter" occurs when an individual is identified as being a positive, inconclusive, or potential match to an individual who has been designated in the TSDB as a known or suspected terrorist. An encounter may be a face-to-face meeting, such as when attempting to enter the United States through a point of entry, being stopped by a local law enforcement officer for a traffic violation, or attempting to travel internationally on a commercial airline. Encounters may also be paper-based, such as when an individual has submitted an application for a visa.

agencies, including the FBI. In addition, individuals are removed from the TSDB once their inclusion is no longer considered warranted.<sup>10</sup>

### **Failed Terrorist Attack of December 25, 2009**

On December 25, 2009, a Nigerian national, often referred to publicly as "the Underwear Bomber," attempted to detonate an explosive device onboard a flight from Amsterdam to Detroit. The flight crew restrained the individual and the plane landed safely. After the plane landed, the perpetrator was taken into custody by the Department of Homeland Security, Customs and Border Protection (CBP) and later questioned by the FBI.<sup>11</sup> The perpetrator of this failed attack was not on the consolidated terrorist watchlist.

As a result of this incident, the White House directed what is known as the Watchlisting Community to examine the government's watchlist processes to identify and correct any weaknesses.<sup>12</sup> This review revealed that the federal government had possessed all of the information necessary to place the perpetrator of the attack on the consolidated terrorist watchlist and prevent him from flying to the United States. Although the individual was in the NCTC's Terrorist Identities Datamart Environment (TIDE), NCTC had not sent the individual's information to the TSC for inclusion on the consolidated watchlist used by screening agencies to identify suspected or known terrorists, the TSDB. This incident highlighted vulnerabilities in the U.S. government's watchlist policies and procedures and led to the issuance of revised watchlist guidance in July 2010.<sup>13</sup>

In this audit, we sought to evaluate the impact on the FBI's watchlisting system of the failed terrorist attack on December 25, 2009. We also assessed the effectiveness of FBI initiatives, implemented between 2009 and 2012, that were intended to ensure the accuracy, timeliness, and completeness of the FBI's watchlisting practices, including watchlist nominations and removals.

### **Overview of the Watchlist Process**

When a law enforcement or intelligence agency identifies information on a known or suspected terrorist, the source agency nominates that person for

---

<sup>10</sup> In fiscal year (FY) 2011, the TSC's screening partners reported more than 1.2 billion queries against the terrorist screening database. According to TSC data, the identities of more than 500,000 persons were included in the TSDB as of September 2012.

<sup>11</sup> The individual ultimately pleaded guilty and is currently serving a life sentence in federal prison.

<sup>12</sup> Members of the Watchlist Community include the Office of the Director of National Intelligence, Central Intelligence Agency, the National Geospatial Intelligence Agency, the National Security Agency, the National Reconnaissance Office, and the Departments of Justice, Defense, State, Treasury, Homeland Security, and Energy.

<sup>13</sup> In March 2013, the Watchlist Community issued revised Watchlist Guidance. Because this new policy document was issued after the scope of this review, we do not address it in this report.



Inclusion in the TSDB.<sup>14</sup> As additional relevant information is obtained that either enhances the identifying information or indicates that the individual has no nexus to terrorism, the record should be either updated or removed.

As shown in Exhibit 1-1, all nominations from source agencies to the consolidated watchlist are vetted through the FBI or NCTC. NCTC is responsible for forwarding to the TSC source agency nominations, including those from the FBI, for international terrorist identities. The FBI is responsible for submitting all domestic terrorist identity nominations directly to the TSC. Although the FBI is a source agency for both domestic and international terrorist information, it forwards relevant information through the NCTC on suspected or known international terrorists.

Analysts at NCTC (for known or suspected international terrorism nominations) and the FBI (for known or suspected domestic terrorism nominations) review the nomination information and decide whether the person is an appropriate candidate for inclusion on the consolidated watchlist. This review includes an evaluation of the information supporting the nomination, an examination of the quality and accuracy of the identifying information, and an examination of whether sufficient identifying information is available. The standard for acceptance of nominations to the TSDB is that there is a reasonable suspicion that the individual is a known or suspected terrorist. From a data perspective, the minimum biographic criteria for inclusion of a terrorist identity into the TSDB are that the record contains a last name and at least one additional piece of identifying information (for example, a first name or date of birth). NCTC and the FBI are responsible for providing the TSC with an unclassified subset of identifying information for individuals known or suspected to be or have been involved in activities related to international or domestic terrorism.<sup>15</sup>

---

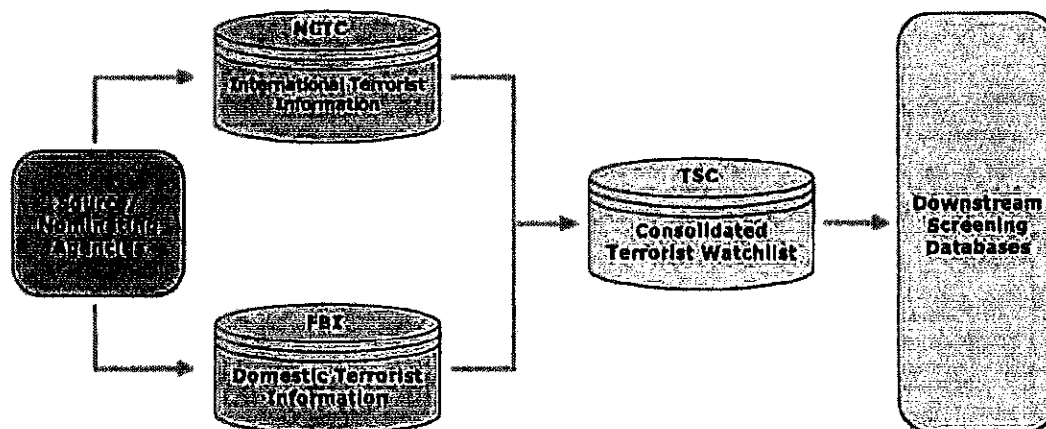
<sup>14</sup> The TSDB is not limited to information about known or suspected terrorists. To facilitate certain screening functions, the TSDB includes information about certain non-terrorists, [REDACTED].

<sup>15</sup> The TSC also has an emergency nomination process, which is used when there is an imminent threat and a watchlist record needs to be created quickly. Under the "expedited" process, a requesting agency informs the TSC directly, and the TSC adds the individual to the consolidated watchlist. The requesting agency then is required to submit a nomination using the standard nomination processes. This emergency process is discussed in more depth in Finding II.

---

**EXHIBIT 1-1**  
**Terrorist Watchlist Dataflow**

---




---

Source: OIG depiction of watchlist process

---

The TSC exports the unclassified terrorist Identity Information contained in the TSDB to other government agency data systems for use during screening activities, such as for the review of passport and visa applications by the State Department and review of international and domestic airline passengers and border crossings by the Department of Homeland Security (DHS), including U.S. Customs and Border Protection (CBP) and the Transportation Safety Administration (TSA). The TSC also provides known or suspected terrorist Identity Information to the FBI for use in name and fingerprint-based identification and background checks conducted by the FBI and other law enforcement entities.<sup>16</sup>

The screening personnel at U.S. points of entry and federal, state, local, territorial, and tribal law enforcement agencies use the watchlist to determine how to handle encounters with known or suspected terrorists. When a name appears to be a match against the terrorist watchlist during screening, requestors receive a return message through their respective agency's screening database informing them of the preliminary match and directing them to call the TSC.

When the TSC is notified of a potential match, TSC staff in the 24-hour operations center assist in confirming the subject's identity by searching the TSDB and supporting databases to locate any additional information that may assist in making a conclusive identification. The caller is immediately informed if the subject of the inquiry does not match the identity of an individual on the watchlist. If the subject of the inquiry is a positive or inconclusive match to a known or suspected terrorist, the FBI's Terrorist Screening Operations Unit (TSOU) is responsible for

---

<sup>16</sup> A description of the downstream screening systems is contained in Appendix II.

coordinating the U.S. government's response.<sup>17</sup> For example, TSOU may deploy agents to interview and possibly apprehend the subject.

Information gathered as a result of the encounter is analyzed for new identifying information about the known or suspected terrorist. Any new information is used to enhance existing watchlist records by means of a modification request. The Intelligence Community and law enforcement personnel use information gathered as a result of encounters with known or suspected terrorists in assessing threats and conducting investigations.

### *The Interagency Process*

The President of the United States ultimately is responsible for making decisions regarding national security, and multiple Executive Branch agencies are involved in ensuring the security of the United States and its citizens, both domestically and abroad. To help ensure that the efforts of government agencies are coordinated and effectively implemented, the United States established the National Security Council (NSC).<sup>18</sup> The NSC serves as the President's principal forum for considering national security and foreign policy matters. It is chaired by the President and is called into session at the President's discretion.

Immediately following the events of September 11, 2001, Congress established the Homeland Security Council (HSC).<sup>19</sup> The HSC is the principal venue for interagency deliberations on issues that affect the security of the homeland, such as weapons of mass destruction, natural disasters, pandemic influenza, terrorism, and watchlisting.

On May 26, 2009, the NSC staff was combined with the HSC staff into the National Security Staff (NSS). The NSS supports all White House policymaking activities related to international, transnational, and homeland security matters, including the watchlisting of known or suspected terrorists. Both the NSC and HSC continue to exist by statute as independent councils of leadership to advise the President.

Each Council has a similar organizational structure, including a Principals Committee, a Deputies Committee, and Interagency Policy Committees.<sup>20</sup>

---

<sup>17</sup> An inconclusive match result occurs when the TSC operations center is not able to positively or negatively conclude that the encountered individual is the same individual on the watchlist. These encounters are forwarded to TSOU for further investigation.

<sup>18</sup> Congress established a formal national security structure that was codified in the National Security Act of 1947. Presidential Policy Directive-1, entitled "Organization of the National Security Council System," was issued on February 13, 2009, to direct the organization of the National Security Council system.

<sup>19</sup> Homeland Security Act of 2002 and Homeland Security Presidential Directive-1, dated October 29, 2001, entitled "Organization and Operation of the Homeland Security Council."

<sup>20</sup> The HSC refers to its policy committees as "Policy Coordination Committees."

The Principals Committees serve as the senior interagency forums for consideration of policy issues affecting national security. Subordinate to the Principals Committees are the Deputies Committees.<sup>21</sup> As senior sub-Cabinet interagency forums, the Deputies Committees are responsible for day-to-day crisis management, directing the work of sub-committees, and ensuring that issues brought before the Principals Committees or the NSC or HSC have been properly analyzed and prepared for deliberations.

Interagency Policy Committees are composed of substantive experts and senior officials from the departments and agencies represented on the Deputies Committees. These policy committees are responsible for managing the development and implementation of national security policies by multiple agencies of the U.S. government and may contain working groups, or sub-Interagency Policy Committees, to help facilitate discussions regarding specific issues.

#### *Terrorist Watchlist Guidance*

To help formalize the U.S. government's watchlisting policies and procedures, the TSC first issued a formal, comprehensive watchlist protocol (Protocol) in July 2007.<sup>22</sup> The Protocol provided the Watchlist Community with specific guidance regarding nominations to the watchlist, including the amount of biographic and derogatory information needed for nominations to the watchlist. The TSC updated and reissued the Protocol in June 2008 and, again, in February 2009.

Following the failed terrorist attack on December 25, 2009, the TSC issued new watchlist guidance to address weaknesses identified during the failed attack and help standardize the watchlist process.<sup>23</sup> For example, the new watchlist guidance provided additional clarification and explanation regarding specific activities, [REDACTED] that a nominating agency should consider in determining whether there is a reasonable suspicion that a person is a known or suspected terrorist. In addition, the watchlist guidance now allows for the inclusion on the watchlist of individuals [REDACTED]

24

<sup>21</sup> The Deputies Committee is composed of the deputy or relevant under secretaries to the Cabinet secretaries.

<sup>22</sup> *Protocol Regarding Terrorist Nominations*, July 2007.

<sup>23</sup> Terrorist Screening Center, *Watchlist Guidance*, July 2010.

<sup>24</sup> [REDACTED]



[REDACTED]

The new guidance initially was approved in May 2010, and issued to the Watchlist Community in July 2010 after a multi-agency classification review and revision process.

### **Overview of Internal FBI Watchlist Processes**

According to the Attorney General Guidelines for Domestic FBI Operations, which became effective on December 16, 2008, the FBI is permitted to use different types of activities to investigate potential violations of federal law and threats to national security, including threat assessments, preliminary investigations, and full investigations. Investigative activity begins at the appropriate level based upon the information known at the time.

- Assessments are the lowest level of FBI investigative activity and do not require a particular factual predication. In short, an Assessment may be conducted when there is reason to collect information or facts to determine whether a criminal or national security threat exists.
- Preliminary investigations are authorized when there exists any allegation or information indicative of possible criminal activity or threats to the national security.
- Full investigations are authorized when there are specific and articulable facts giving reason to believe that a criminal activity or a threat to national security may exist.<sup>25</sup>

To be nominated to the watchlist, subjects of FBI terrorism investigation must meet the "reasonable suspicion" standard. To meet this standard, the FBI must have "articulable" intelligence or information which, based on the totality of the facts, and taken together with rational inferences from those facts, reasonably warrants a determination that the subject is known or is suspected to be (or has been) knowingly engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism or terrorist activities.

According to the TSC Chief Counsel, subjects of FBI preliminary investigations may not necessarily meet the reasonable suspicion threshold required for watchlisting. However, she indicated that subjects of full terrorism investigations will always meet the reasonable suspicion standard for watchlisting because of the criteria for expanding a preliminary to a full investigation.

---

<sup>25</sup> This description is not intended to be a comprehensive discussion of the myriad policies criteria pertaining to authorized FBI investigative activity. This is intended to provide a broad framework for the different levels of investigative activity and to provide context for the FBI's watchlist nomination requirements.



FBI policy requires that subjects of preliminary or full domestic and international terrorism investigations be forwarded to FBI headquarters for potential watchlisting.<sup>26</sup> Subjects of assessments are not to be submitted for watchlisting.

Under certain circumstances, FBI policy also allows for the nomination of known or suspected terrorists for whom the FBI does not have an open terrorism investigation. For example, foreign governments occasionally provide the FBI with terrorism information about an individual, who may be nominated to the watchlist if the FBI determines that they present a threat to national security. Generally, if the individual is located abroad and the FBI believes the individual meets the criteria for watchlisting, the FBI's nomination follows the FBI's procedures for nominating a non-investigative subject. We discuss the FBI's policy and procedures for non-investigative subjects in Finding III of this report.

#### *Watchlist Nomination Process*

When an FBI field division opens a terrorism investigation, the field division must notify FBI headquarters within 10 business days of the initiation of the investigation. One of the FBI headquarters' units that must be notified is the FBI's Terrorist Review and Examination Unit (TREX). TREX is the FBI headquarters unit that serves as the processing center for FBI watchlist nominations resulting from open FBI terrorism investigations. If sufficient identifying information on the subject exists to support a watchlist nomination, the field division is required by FBI policy to nominate the subject for entry into the TSDB. Generally, a [REDACTED] are required for FBI nominations to the consolidated watchlist.

As shown in Exhibit 1-2, the field division is required to submit the nomination to TREX. In order for TREX to process an initial watchlist nomination, the assigned case agent must electronically submit copies of the opening electronic communication document and a watchlist nomination form.<sup>27</sup> Once the field division submits the watchlist nomination, TREX is responsible for reviewing and approving nominations for both international and domestic terrorist nominations. Upon receiving the complete nomination package, a TREX Technical Information Specialist (TIS) reviews the nomination form, the opening electronic communication, and additional documentation to verify that justification for the nomination exists, that the information submitted is accurate and complete, and that the criteria are met for inclusion of the subject in downstream databases. If

<sup>26</sup> Prior to December 2009, the FBI's policy stated that known or suspected domestic terrorism subjects of preliminary investigations could be nominated to the watchlist at the discretion of the responsible FBI Field Division. On December 7, 2009, the FBI revised its policy to require the nomination of subjects of domestic terrorism preliminary investigations who met the criteria for nomination to the TSDB. FBI policy permits the exclusion from the watchlist of subjects of full domestic terrorism investigations that focus on groups or organizations that are involved in national security threats to the public.

<sup>27</sup> The same form is used for initial nominations to the watchlist, modifications of watchlist records, and watchlist record removals. Throughout this report, we refer to this form in the context of its intended capacity as the nomination, modification, or removal form.

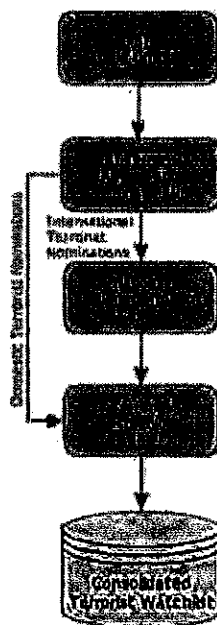
there is insufficient information, TREX follows up, including contacting the nominating agent or field division to request additional information.

Once TREX has reviewed and approved a watchlist action, it sends the actions for known or suspected *international* terrorists to the NCTC branch staffed by FBI personnel. The nomination process for known or suspected *domestic* terrorists differs in that TREX submits these nominations directly to the TSC. The NCTC is not involved in the process because its TIDE database is prohibited from containing purely domestic terrorism information. FBI policy requires that TREX process watchlist nominations within 5 business days of receipt of a complete nomination package from the field division.

The FBI analysts assigned to the NCTC enter the subject's information into NCTC's TIDE database. An NCTC supervisor conducts an additional quality assurance review to confirm the analyst's entry of data is complete and accurate by comparing the nomination to the supporting paperwork before releasing the records for export to the TSC. According to NCTC management, NCTC's standard is to process these nominations within 24 hours.

The TSC then performs one final quality review of the new records before importing them into the TSDB. The TSC exports the watchlist information to the various screening databases used by the U.S. government and some of its allies. The TSC's standard is to perform this check and complete the processing of the nominations within 24 hours.

**EXHIBIT 1-2**  
**FBI Watchlist Nomination Process**  
**for FBI Terrorism Investigation Subjects**



Source: OIG depiction of the FBI watchlist process

Similarly, when the FBI closes a terrorism investigation, FBI policy generally requires that the subject of the closed investigation be removed from the consolidated terrorist watchlist. However, in limited circumstances the FBI may leave a subject on the watchlist after the case has closed. These watchlisted individuals are referred to as non-investigative subjects. For example,

[REDACTED]. However, the FBI may believe that the individual still poses a threat to national security and warrants continued watchlisting.

***Watchlist Removal Process***

The removal process mirrors the nomination process. The FBI case agent is required to prepare a removal form that is electronically submitted to TREX. TREX reviews and approves the removal form and forwards international terrorist record removals to NCTC for entry into the TIDE database, which in turn exports the removal to the TSC. Domestic terrorist record removals are sent directly to the TSC. The TSC imports the removal information into the consolidated terrorist

watchlist, thus removing the record from the watchlist and the associated downstream screening databases that are populated from it.<sup>28</sup>

### **Previous OIG Reviews**

Since the creation of the TSC, the OIG has conducted several watchlist-related audits, including three audits of the TSC and one each of DOJ and FBI watchlist processes.<sup>29</sup> In our two most recent audits, we examined the internal watchlist processes for DOJ and the FBI.<sup>30</sup> In these two audits, we found that DOJ and the FBI: (1) failed to nominate to the watchlist subjects of terrorism investigations, (2) failed to remove from the watchlist subjects of closed terrorism investigations, (3) completed nominations to the watchlist in an untimely manner, and (4) used non-standard processes to nominate individuals who were not the subject of an FBI investigation or "non-investigative subjects."

As a result, we recommended to the FBI that it evaluate its overall nomination process, determine the total amount of time that is needed and can be afforded to the process, and determine how much time should be allocated to each phase of the process. In addition, we recommended that the FBI reexamine its watchlisting policies and practices during the case closure and watchlist removal process to ensure that they are clear and appropriate. We also recommended that the FBI evaluate its watchlist policy and procedures for non-investigative subjects.

In this audit, we examine several corrective actions that were implemented by the FBI in response to these two most recent audits. The results of our analysis are contained in Finding II and Finding III of this report.

28



<sup>28</sup> See Appendix III for a summary of these reports, including our findings and recommendations.

<sup>30</sup> U.S. Department of Justice Office of the Inspector General, *DOJ Terrorist Watchlist Nomination Processes*, Audit Report 08-16 (March 2008) and *FBI's Terrorist Watchlist Nomination Practices*, Audit Report 09-25 (May 2009).



## OIG Audit Approach

The preliminary objectives of this audit were to: (1) evaluate the impact on the FBI's watchlisting system of the failed terrorist attack on December 25, 2009, and (2) assess the effectiveness of FBI initiatives, implemented between 2009 and 2012, that were intended to ensure the accuracy, timeliness, and completeness of the FBI's watchlisting practices, including watchlist nominations and removals.

To accomplish these objectives, we conducted over 80 interviews of employees and officials at FBI headquarters and FBI field divisions as well as NCTC and TSC personnel who are involved in the processing of nominations to the consolidated terrorist watchlist. Findings I through III provide the results of our audit.

In Finding I, we chronicle the TSC's actions taken following the failed terrorist attack on December 25, 2009. This includes an in-depth discussion of the TSC's actions taken regarding temporary modifications to the watchlist status for several groups of individuals. In this finding, we also assess policy and procedural weaknesses that occurred while the TSC effected the modifications.

Finding II focuses on our assessment of the effectiveness of the initiatives implemented by the FBI in response to our prior audits to ensure the accuracy, timeliness, and completeness of the FBI's watchlisting practices, including watchlist nominations and removals. This included reviewing policies and processes concerning FBI nominations to and removals from the terrorist watchlist and performing tests of watchlist nomination and removal data submitted by four FBI field divisions: Chicago, Illinois; Los Angeles, California; Miami, Florida; and Minneapolis, Minnesota.<sup>31</sup> Further, we reviewed the FBI's controls over nominations to the watchlist that are submitted using the "expedited" nomination process, without initially going through the NCTC.

In Finding III, we examined the FBI's processes for and internal controls over watchlist records for non-investigative subjects, including changes the FBI made in this area following our previous audits. This included a review of the FBI's processing of a judgmental sample of 70 requests to nominate to or retain non-investigative subjects on the watchlist. For each sampled case, we analyzed documentation at TREX, the FBI's International and Domestic Terrorism Units, and the TSC to determine whether the nomination was submitted and processed in accordance with FBI policy, whether the subject was appropriately nominated to or retained on the watchlist and, when appropriate, whether the subject was removed from the watchlist in a timely manner.<sup>32</sup>

---

<sup>31</sup> To compare the FBI's processing of watchlist actions, we selected three of these offices because they were included in our testing during our prior audit – Los Angeles, Miami, and Minneapolis. Appendix I contains an expanded discussion of the audit's scope and methodology.

<sup>32</sup> The FBI's International and Domestic Terrorism Units are the FBI headquarters units that are responsible for providing operational support and coordination for FBI counterterrorism investigations.



Appendix I contains further description of our audit objectives, scope, and methodology.

## **FINDINGS AND RECOMMENDATIONS**

### **I. TSC ACTIONS FOLLOWING THE FAILED TERRORIST ATTACK OF DECEMBER 25, 2009**

In the immediate aftermath of the failed terrorist attack on December 25, 2009, the TSC was directed through an interagency process to make a series of temporary modifications to the watchlist status for several groups of individuals. These changes reflected concern over emerging threat information and were not covered by the then-existing watchlist protocol and procedures. Despite these shortcomings in the protocol and other technical and procedural issues it encountered, we found that, overall, the TSC responded commendably to the attempted terrorist attack. However, we determined that because of the policy, technical, and procedural issues, the TSC was unable to readily identify individuals who met the threat-based criteria, or to easily generate a listing of all of the records modified in response to the directions received following the December 25, 2009, incident. As a result, the TSC relied on largely manual processes to track the watchlist modifications and associated in-depth ("deep dive") reviews of affected watchlist records. The TSC and the Watchlist Community have developed new policy and procedures to respond to a similar event in the future. Following these procedures should help to ensure that future threat-based watchlist modifications are communicated more effectively and coordinated more efficiently. We recommend that the TSC implement procedures for comprehensively documenting its watchlist-related actions during crisis or other situations calling for expedited actions. In addition, the TSC should continue to improve the TSDB to allow the TSC to more efficiently identify individuals who meet threat-based criteria and to track the resulting modifications of watchlist records.

#### **TSC Actions Following the Terrorist Attack**

On December 25, 2009, at approximately 12:25 p.m., a Nigerian national attempted to detonate an explosive device onboard a flight from Amsterdam to Detroit. According to TSC documentation, TSC's operations center was notified of the attempted terrorist attack at 12:46 p.m., via an e-mail from the CBP's National Targeting Center.<sup>33</sup> The TSC operations center immediately notified

---

<sup>33</sup> The National Targeting Center (NTC) is part of DHS. It provides around-the-clock tactical targeting and analytical research in support of the anti-terrorism efforts of DHS's Customs and Border Protection.

the TSC Director.<sup>34</sup> The TSC Director subsequently notified FBI executive management.

According to the TSC Director, numerous meetings and telephone calls were held on December 25, 2009, among counterterrorism stakeholders throughout the Executive Branch and the Administration. During one of these meetings, the TSC was directed to modify the watchlist status of certain individuals to address potential threats based on emerging information.

Although the TSC Director did not attend the meeting noted above, the TSC Director said that he had discussed the proposed changes with FBI executive management who attended the meeting. At approximately 6:50 p.m. on December 25, 2009, NCTC called the TSC to convey the modification request. The request entailed modifications to watchlist statuses that were not covered by the then-current watchlist protocol.<sup>35</sup> The modifications initially were intended to be in effect [REDACTED].

The watchlist status modifications, which were made between December 25, 2009, and February 1, 2010, related to: individuals with a nexus to three specific countries who also met certain other criteria, individuals with [REDACTED] who were in TIDE but not watchlisted in the TSDB as of December 25, 2009, all detainees from Guantanamo Bay, and individuals affiliated with two specific countries. These are discussed in the sections below.

#### *Target Country Upgrades - December 25, 2009*

On December 25, 2009, the TSC reported that NCTC requested that the TSC upgrade to the TSA Selectee List watchlisted [REDACTED].<sup>36</sup> In addition to the individuals watchlisted at the time that met these threat-based criteria, NCTC requested that the TSC upgrade to the TSA Selectee List persons that met the threat-based criteria and who had *not been watchlisted* (in the TSDB) prior to December 25, 2009, but who were included in NCTC's TIDE.<sup>37</sup>

---

<sup>34</sup> The TSC operations center notified other TSC managers about the incident at approximately 3 p.m.

<sup>35</sup> Protocol Regarding Terrorist Nominations, February 2009.

<sup>36</sup> These individuals generally did not meet the existing criteria for placement on the TSA Selectee or No Fly Lists. The TSA Selectee List requires that individuals be subject to enhanced screening before being allowed to fly on a commercial airline. As noted previously, individuals on the No Fly List are not permitted to board a commercial flight.

<sup>37</sup> According to the TSC, these individuals had not been previously uploaded from TIDE to the TSDB because they did not meet the minimum biographic or derogatory information criteria for inclusion in the consolidated watchlist.

The TSC identified [REDACTED] identities that were in the TSDB at that time and met the threat-based criteria.<sup>38</sup> According to TSC documents, the TSC forwarded these records in a spreadsheet by 11 p.m. on December 25, 2009, to NTC and the Transportation Security Administration (TSA) Office of Intelligence for processing and dissemination to the airlines.<sup>39</sup> TSA reported that the records would be made available to the airlines [REDACTED].

*Target Country Upgrades – December 26 through December 31, 2009*

The next day, December 26, 2009, the TSC discovered that it failed to include in the original spreadsheet sent to TSA records for watchlisted individuals with a nexus to [REDACTED]

[REDACTED].<sup>40</sup> As a result, on December 26, the TSC generated a more complete listing of TSDB records fitting the declared criteria, and the TSC identified approximately [REDACTED] responsive watchlist records.<sup>41</sup> That same day, the TSC provided the listing of watchlist records to the TSA's Office of Intelligence, as well as the Secure Flight program.<sup>42</sup> According to the TSC, Secure Flight was able to process the records. However, TSA's Office of Intelligence was unable to process such a large volume of records and requested a smaller list of watchlist

<sup>38</sup> For both of the upgrade populations (the TSDB watchlisted individuals and those individuals included in TIDE but not TSDB), [REDACTED]

[REDACTED]. According to the TSC, the range was broadened to help ensure that individuals posing a potential terrorist threat were nominated to the watchlist and upgraded to the Selectee List. Because the upgrade of individuals included in TIDE but not the TSDB was not completed until a later time, that action is discussed in the following section.

<sup>39</sup> The TSC's customary practice for such watchlist modifications would be to modify the individual watchlist record within the TSDB to reflect the upgrade to the Selectee List. The modified records would then be exported to the TSA for vetting against passenger data. [REDACTED]

[REDACTED]. On December 31, 2009, the TSC modified the watchlist status in the TSDB for records that contained sufficient biographical information.

<sup>40</sup> [REDACTED]

<sup>41</sup> The reported figure represents the number of *watchlist records* that met the stated criteria. This does not equate to the number of known or suspected terrorists as a single person may have multiple records to account for the use of aliases, alternate identities, and multiple identifying documents. As such, the number of watchlist records generally will be larger than the number of suspected or known terrorists.

<sup>42</sup> Secure Flight is the system used by the TSA to identify individuals that may pose a threat to aviation. Prior to the implementation of Secure Flight, individual airlines were responsible for pre-flight watchlist screening for domestic flights, and CBP was responsible for pre-flight watchlist screening for international flights. In November 2010, TSA Secure Flight assumed full responsibility for pre-flight watchlist screening of passengers on domestic and international flights into, out of, and within the United States. Secure Flight now collects passenger information submitted by the airlines for domestic and international flights and vets it against the watchlist. Secure Flight results are then transmitted back to the airline. This process serves to prevent individuals on the No Fly List from boarding an aircraft and to identify individuals on the Selectee List for enhanced screening.

records. TSC analysts reviewed the list of [REDACTED] records and selected the first watchlist record for each identity. On December 28, the TSC provided the TSA's Office of Intelligence with a spreadsheet containing [REDACTED] watchlist identities.

On December 29, 2009, the TSC again learned that the spreadsheet of watchlisted individuals it had provided to the TSA's Office of Intelligence was incomplete, as it did not contain records for [REDACTED]. The TSC retransmitted a complete listing of [REDACTED] watchlist identities to the TSA's Office of Intelligence.

For individuals meeting all threat-based criteria who were in TIDE but not in the TSDB, on December 27, 2009, the TSC received from NCTC a data file containing the nominations to the watchlist for [REDACTED] and [REDACTED] identities. On December 31, 2009, NCTC provided TSC with the data file of nominations for inclusion on the Selectee List of [REDACTED] identities who met all threat-based criteria but had not been watchlisted prior to December 25, 2009. The TSC processed both of the data files of nominations from NCTC using TSC normal business processes and exported the nominations to DHS's TECS and TSA's Office of Intelligence and Secure Flight on the day received.<sup>43</sup>

On December 31, 2009, NCTC advised the TSC that DHS had requested that [REDACTED] be added to the list of target threat countries. According to the TSC Director, the TSC processed nominations of [REDACTED] who were in TIDE but who had not been watchlisted prior to December 25.

#### *Target Country Upgrades – January 2010*

According to a TSC official, at the beginning of January 2010, there were some questions at the TSC regarding the targeted upgrading of watchlist records. In addition, the TSC Director and TSC Chief Counsel said that on January 4, 2010, they became concerned about the lack of written direction regarding the modification of the watchlist status beyond the initially agreed upon timeframe of [REDACTED]. Because the requested upgrades were not covered under the existing watchlist protocol and because the TSC had not received any formal, written guidance, the TSC Director and Chief Counsel informed the FBI General Counsel of the directives and the lack of supporting documentation.

The TSC Director said that the FBI General Counsel advised that the FBI believed that the directions to modify the watchlist status of the certain individuals

---

<sup>43</sup> The TECS System (which is no longer an acronym) serves as the principal information system supporting border management and the law enforcement mission of DHS CBP and other federal law enforcement agencies.



were permissible under Homeland Security Presidential Directive-6 (HSPD-6).<sup>44</sup> The FBI General Counsel also advised that the modifications should be continued despite the TSC not having the direction in writing. As a result, the TSC Director began to confirm in writing the directions provided to the TSC and the actions taken by the TSC.<sup>45</sup>

In response, the TSC was asked to wait to remove the individuals until the Interagency group met on January 15, 2010, and discussed the merits of either retaining or removing the individuals from the watchlist. The TSC was also told that the TSC or NCTC could remove or modify the status of individuals on a case-by-case basis.<sup>46</sup>

On January 6, 2010, the TSC received an e-mail that indicated there appeared to be some confusion regarding the scope of the direction to watchlist certain groups of individuals who did not meet the watchlist criteria, had not been watchlisted prior to December 25, 2009, but were known to the U.S. Intelligence Community and were included in TIDE. Specifically, the e-mail said that, through the interagency process, NCTC was asked to review certain groups of individuals in TIDE to determine if they should be temporarily watchlisted based on information about emerging threats. The e-mail indicated that the final decision on individual upgrades was deferred to NCTC professionals who "do this for a living." The e-mail continued on to discuss a separate and distinct DHS request to receive a full listing of all individuals in TIDE regardless of their watchlist status.

We discussed this e-mail with TSC officials because it could be read to say that the TSC had not been specifically requested to upgrade the watchlist records but only had requested that NCTC review the categories of individuals and determine if the watchlist statuses should be modified. The TSC Director told us that he was confident that he fully and clearly understood the Interagency process requests and that the TSC had carried out the modifications exactly as they had been requested. The TSC Director stated that he believed that the confusion

---

<sup>44</sup> On September 16, 2003, the President signed Homeland Security Presidential Directive-6 (HSPD-6), requiring the establishment of an organization to "consolidate the Government's approach to terrorism screening and provide for the appropriate and lawful use of Terrorist Information in screening processes." Subsequently, the Attorney General created a new organization, the TSC, to consolidate terrorist watch lists and provide 24-hour, 7-day a week operational support for federal, state, local, territorial, tribal, and foreign government as well as private sector screening across the country and around the world.

<sup>45</sup> In the TSC Director's initial e-mail dated January 6, 2010, he confirmed the verbal directions that the records remain at the current watchlist status for [REDACTED].

<sup>46</sup> On January 15, 2010, an Interagency committee requested these individuals be re-watchlisted. According to the TSC, between January 5 and January 15, 2010, [REDACTED] of the original [REDACTED] were dewatchlisted because there was insufficient derogatory information to support watchlisting. Either due to additional information being added to the records or subsequent direction from the interagency process, [REDACTED] dewatchlisted individuals were renominated to the watchlist through the TSC's normal business process between February 4 and February 15, 2011. A total of [REDACTED] identities do not appear to have been renominated.

referred to in the e-mail stemmed from the similar but separate tasks being requested. We believe that because the watchlist upgrade requests were not in writing, the situation was ripe for misinterpretation or confusion and increased the risk that the modifications would not be implemented as intended and could have caused delays in carrying out the directions. At our audit close-out meeting and in subsequent communications, the TSC stressed that as a result of this increased risk, officials took the initiative to document the direction they received through official correspondence.

#### **Upgrades**

As a result of an interagency meeting on January 11, 2010, NCTC and the TSC were directed to temporarily include on the TSA No Fly List all individuals in TIDE (including those already in the TSDB and those existing in TIDE but not watchlisted) with [REDACTED]. On January 16, 2010, the TSC identified [REDACTED] persons with [REDACTED] who were already watchlisted and included these individuals on the No Fly List. In addition, NCTC identified [REDACTED] persons with [REDACTED] who were not previously watchlisted but had been included in TIDE.

According to the TSC, many of the persons watchlisted and upgraded to the No Fly List were individuals without any information indicating a personal involvement in terrorism, [REDACTED].<sup>47</sup> As such, many of these [REDACTED] did not meet either the current substantive criteria for placement on the No Fly List or the minimum substantive derogatory information requirement for inclusion in the TSDB.

When the NCTC provided to the TSC the records for [REDACTED], the TSDB's business rules automatically excluded the records from inclusion in the TSDB.<sup>48</sup> According to NCTC, to bypass the TSDB business rules and include these individuals in the TSDB, NCTC proposed assigning an unused and obsolete code to the records. However, the TSC Director said that the proposed code denoted that the subject had engaged in unlawful acts. As a result, if the individual were encountered by a CBP agent at the border, the agent could erroneously believe that the person had engaged in criminal activity.

The TSC explored alternative ways to upgrade the [REDACTED] in TIDE to the No Fly List. To meet the directive to modify the watchlist records of [REDACTED] without erroneously labeling individuals as having engaged in criminal conduct, the TSC provided TSA with a spreadsheet containing the persons with [REDACTED]

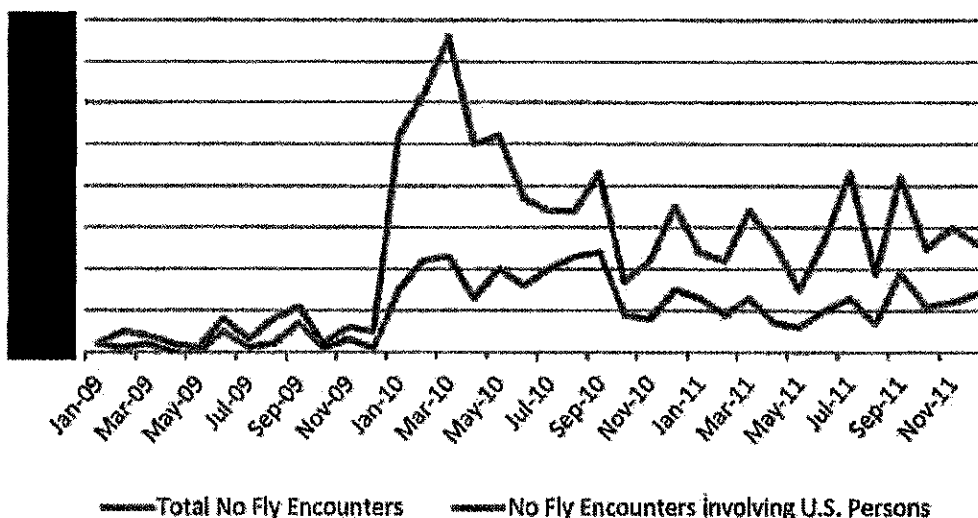
<sup>47</sup> [REDACTED]

<sup>48</sup> A business rule is an automated information technology function in which the record is analyzed for specific deficiencies and compliance with criteria.

██████████ who had not been previously watchlisted.<sup>49</sup> In this manner, these individuals were added to the No Fly List, without being added to the TSDB.

As shown in Exhibit 2-1, as a result of the inclusion on the No Fly List of individuals with ██████████, the TSC experienced a surge in the number of encounters with individuals on the No Fly List. As a result, the TSC was required to expend more resources responding to these encounters.

**EXHIBIT 2-1**  
**Encounters With Persons on the No Fly List**  
(January 2009 through December 2011)



Source: Terrorist Screening Center

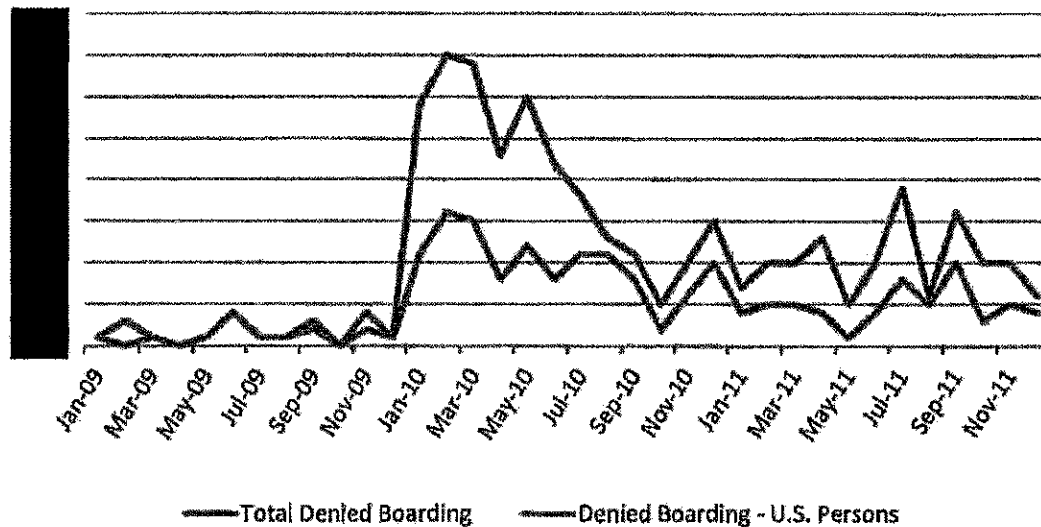
As part of the interagency process, the TSC Director reported that the TSC had a significant number of encounters ██████████ who experienced difficulty traveling because of their new No Fly status. Moreover, for some of the individuals encountered, the U.S. government possessed minimal information to support watchlisting. The TSC Director said that with each No Fly encounter, he personally reviewed the available information and, when appropriate, approved downgrading the individual from the No Fly to the Selectee List.

As shown in Exhibit 2-2, U.S. citizens and legal permanent residents who were on the No Fly List also experienced problems with airline travel. U.S. Persons generally have a right to return to the United States and placement on the No Fly

<sup>49</sup> The TSC would normally modify the individual watchlist record within the TSDB to reflect the nomination to the No Fly List. The modified records would then be exported to the TSA for vetting against passenger data.

List does not bar an individual from entering the United States.<sup>50</sup> The TSC reported that from January 1, 2010, to April 20, 2010, [REDACTED] who were on the No Fly List were denied boarding airline flights bound for the United States.<sup>51</sup>

**EXHIBIT 2-2**  
**Persons on the No Fly List**  
**Who Were Denied Boarding an Aircraft**  
**(October 2009 through December 2011)<sup>52</sup>**



Source: Terrorist Screening Center

As a result, on January 19, 2010, the Terrorist Screening Center Policy Board Working Group met to discuss the No Fly upgrades of [REDACTED]

<sup>50</sup> The U.S. government has the authority to bar a person on the No Fly List from boarding an aircraft bound for the United States. To help facilitate the return of U.S. Persons denied boarding overseas, the TSC developed an assessment process to determine whether the individual was still appropriately watchlisted [REDACTED]

[REDACTED]. Non-U.S. Persons and those U.S. Persons deemed ineligible for air travel must find alternate methods for traveling, such as boats and automobiles.

<sup>51</sup> [REDACTED]

<sup>52</sup> The TSC provided the OIG with this data on several occasions. This is the information it now asserts is correct.



██████████.<sup>53</sup> The Working Group met again on January 21, 2010, and reached a consensus regarding more specific criteria to guide the decision to either retain Individuals on the No Fly List or downgrade Individuals to the Selectee List. Based on the recommendations from the TSC Policy Board, on January 22, 2010, the original directive for ██████████ was revised and the TSC was provided with more specific guidance as to whether to retain Individuals on the No Fly List or downgrade them to the Selectee List. The TSC reported that on January 24, 2010, it completed its initial review of the watchlist records for the ██████████ and modified each affected person's watchlist status in accordance with the new guidance.

#### *Guantanamo Bay Detainees*

In a January 15, 2010, letter, the TSC Director advised that the TSC had placed all detainees held at the Naval Station, Guantanamo Bay, Cuba, on the No Fly List, as had been required by law.<sup>54</sup>

#### *Individuals Affiliated with Two Specific Countries – January 2010*

Around January 11, 2010, as part of the Interagency process, the TSC was directed to review all existing records in TIDE that had a ██████████ and upgrade the Individual to the No Fly List.<sup>55</sup> In an e-mail dated January 14, 2010, the TSC Director requested written guidance regarding the scope of the watchlist modification directions. The TSC Director expressed his concern that the TSC was receiving a lot of direction and that the message might be getting confused and inaccurate. On January 22, 2010, the TSC received an e-mail that this particular direction would be discussed during an Interagency committee meeting scheduled to occur that day. During that meeting the TSC was provided with more specific guidance on issues raised by the TSC.

The TSC reported that it forwarded all ██████████ persons in TIDE with ██████████ to the TSDB, upgraded existing known or suspected ██████████ terrorists who were already in the TSDB to the No Fly List, and placed ██████████ of known or suspected ██████████ terrorists or those with ██████████ on the Selectee List. According to the TSC,

<sup>53</sup> Generally, the purpose of the TSC Policy Board is to formulate recommendations to the interagency working group concerning government-wide policy guidance for the nomination and watchlisting of, and the management of encounters with known or suspected terrorists. The Policy Board is chaired by the Director of the TSC and composed of senior executive representatives from the Office of the Director of National Intelligence, the Central Intelligence Agency, NCTC, FBI, TSC, and Departments of State, Treasury, Defense, Justice, and Homeland Security. Following the failed terrorist attack on December 25, 2009, the TSC Policy Board made recommendations to the interagency working group on watchlisting issues.

<sup>54</sup> P.L. 111-83 (October 28, 2009), Section 553, codified at 49 U.S.C. 44903(j)(2)(C)(v).

<sup>55</sup> ██████████



the TSC and NCTC identified approximately [REDACTED] individuals with [REDACTED], respectively, who met the stated minimum biographical criteria. An additional [REDACTED] persons had [REDACTED] for a combined total of approximately [REDACTED].

On February 1, 2010, approximately [REDACTED] of these persons were placed on the No Fly List and [REDACTED] persons were placed on the Selectee List. However, for an additional [REDACTED] persons there was insufficient biographic information; for example, [REDACTED]. As a result, these persons could not be upgraded to the Selectee or No Fly Lists.

### **In-Depth Record Reviews ("Deep Dives")**

According to the TSC Director, the Intelligence and Watchlist Communities agreed that, following the initial watchlist additions and modifications, officials would need to thoroughly review each resulting record change to determine the individual's appropriate watchlist status. As a result, the FBI and other Intelligence Community members were directed to review the information in their possession about each individual, determine the appropriate individualized watchlist status, and provide their recommendations to the TSC. The TSC was directed to coordinate the review and effect the necessary changes. According to TSC officials, they compiled the list of persons whose watchlist status was altered as a result of each of the various initiatives following December 25, 2009.<sup>56</sup> They then provided the lists to the reviewers for action.

As shown in Exhibit 2-3, the TSC tracked and monitored the status of what were called "deep dive reviews" of individuals whose watchlist status was altered as a result of the events on December 25, 2009. The reviews began when the TSC provided the lists of affected persons to the reviewers in June 2010. These reviews were not completed until December 2011 – nearly 2 years after the watchlist statuses were altered.<sup>57</sup>

In February 2010, the TSC provided to the deep-dive reviewers the lists of [REDACTED] whose watchlist status was altered in early January 2010. The TSC reported that these deep dive reviews were completed by June 25, 2010, and the TSC made all necessary watchlist status modifications or removals according to each individual's eligibility. For the individuals [REDACTED] whose watchlist status was altered in February 2010, the TSC provided to the deep-dive reviewers the lists of affected individuals within 30 days of the watchlist

---

<sup>56</sup> We identified inconsistencies within TSC documentation regarding the number of individuals whose watchlist status was modified. We discuss this further in the following section entitled "TSC Documentation Supporting Watchlist Modification."

<sup>57</sup> According to the TSC, individuals' watchlist statuses generally were not modified until the deep dive reviews were completed. If an individual was encountered while this was pending the TSC reviewed the nature of the derogatory information and made adjustments in watchlist status, when necessary. Most of the watchlisted subjects were not encountered while their watchlist status was being reviewed.

upgrades. However, the agencies did not complete the deep dive reviews until June 2011.

**EXHIBIT 2-3**  
**Watchlist Status Modification Initiatives and**  
**Related Deep Dive Reviews<sup>58</sup>**

Initiative Description	Total Persons	Date Review Initiated	Deep Dive Completion Date
UPGRADE TO SELECTEE: Previously watchlisted [REDACTED] [REDACTED]	[REDACTED]	6/18/2010	12/07/2011
UPGRADE TO SELECTEE: Not previously watchlisted [REDACTED] [REDACTED]	[REDACTED]	6/18/2010	12/07/2011
UPGRADE TO NO FLY/SELECTEE: [REDACTED]	[REDACTED]	2/8/2010	06/25/2010
UPGRADE: (1) Previously watchlisted [REDACTED] [REDACTED] individuals upgraded to No Fly and (2) Not previously watchlisted [REDACTED] Individuals added to watchlist and upgraded to Selectee	[REDACTED]	2/25/2010	06/30/2011

Source: Terrorist Screening Center

We discussed the deep dive reviews with the TSC Chief Counsel who acknowledged that they took a long time to complete. She said that the watchlist modifications made following the December 25, 2009, incident had been intended to mitigate the potential for another attack and resulted in a significant number of individuals having their watchlist status altered. Because the majority of these individuals were [REDACTED], the increased workload resulting from the deep dive reviews fell primarily to agencies other than the FBI. The TSC Chief Counsel stated that these agencies did not have sufficient resources to review historical records for the number of individuals upgraded in a more timely fashion.

The TSC Director said that he was especially concerned about the operational impact posed by the upgrades [REDACTED] to the No Fly List. Many of these individuals did not qualify for inclusion in the watchlist, much less elevation to

<sup>58</sup> All numbers are approximate counts of persons. For a more detailed analysis of the results of the deep dive reviews, please see Appendix IV.

the No Fly List, based upon the criteria that previously were in place. Because these individuals [REDACTED], they were more likely to travel and be encountered.<sup>59</sup> Although the TSC complied with the initial direction and promptly upgraded these individuals to the No Fly List, the direction did not define the amount of time the upgrades would last. Moreover, the direction did not provide the TSC with guidance regarding the criteria and procedures for reviewing these records until after the TSC experienced a surge in the number of encounters with individuals on the No Fly List. Once it received the guidance and results of the in-depth reviews conducted by others in the Watchlist Community, the TSC worked to quickly process the necessary adjustments to the watchlist records for the [REDACTED]. However, as noted above, the process of completing the deep dive reviews of the individuals with altered watchlist statuses resulting from the other initiatives took much longer to complete.

According to the TSC Chief Counsel, the then-existing watchlist guidance did not contain instructions on how to handle such immediate, threat-based watchlist status changes for whole categories of individuals. Following the December 25 events, the White House directed the TSC to develop recommendations on whether adjustments should be made to the watchlisting nomination criteria, including the biographic and derogatory criteria for inclusion in TIDE, TSDB, the No Fly List, and the Selectee List.<sup>60</sup> During the resulting discussions, new policy was developed to govern the types of temporary upgrades to the consolidated watchlist and No Fly and Selectee Lists that were made following the attempted plane bombing on December 25, 2009.

[REDACTED]

[REDACTED]

<sup>59</sup> As previously discussed, if the individual was encountered, the TSC reviewed the nature of the derogatory information and made adjustments in watchlist status, when necessary.

<sup>60</sup> We discuss the review led by the TSC in greater detail later in this finding.



### **TSC Documentation Supporting Watchlist Modification**

TSC officials told us that the TSC did not document completely its actions with respect to the watchlist status modifications in the early days following the failed terrorist attack on December 25, 2009. The officials attributed some of the difficulty to the need to focus on operational concerns during the immediate crisis situation. As a result, the TSC struggled to reconstruct its actions and was unable to provide us with a complete listing of all the records that were modified during the earliest days following the attack. Because the modifications did not meet the watchlist guidance then in effect and the TSC did not have written confirmation of the directives, we believe that the TSC should have been more vigilant in retaining the necessary evidence to document its actions.

We were told by the former TSC Administrative Unit Chief that he recognized that there was a gap in the TSC's operational documentation. As a result, he directed his administrative staff to begin compiling the necessary documentation to assist executive and operational staff, and this documentation was included as attachments to an electronic communication dated February 17, 2010. The electronic communication contains a summary and numerous attachments that document the TSC's actions as of February 17, 2010, including the number and types of records modified and the dates the modifications occurred. However, it does not contain documentation regarding subsequent key decisions and actions taken by the TSC, such as its involvement in the deep dive reviews. Also, we found that the communication and its attachments had several internal inconsistencies regarding the number and types of records modified, the dates the TSC received the directions regarding those modifications, and the dates the modifications occurred.

In addition, the TSC's Nominations and Data Integrity Unit (NDIU) prepared two additional electronic communications, dated October 5, 2010, and December 17, 2010, respectively, in which it summarized information related to the status of the deep dive reviews.<sup>61</sup> In addition to information on the status of the deep dive reviews, these two electronic communications contained similar information to the February 2010 electronic communication, including the number and types of records modified and the dates the modifications occurred. However, these two electronic communications only contain summary information and do not contain a comprehensive explanation regarding the watchlist modifications, including how the numbers related to each other and how they evolved as tasks

---

<sup>61</sup> The Nominations and Data Integrity Unit (NDIU) is the TSC unit responsible for ensuring the quality and accuracy of the watchlist.



were completed. In addition, the electronic communications did not contain the documents used by the TSC to track its actions related to the deep dive reviews, including spreadsheets and charts.

Moreover, when we reviewed the three electronic communications from February, October, and December 2010, we found significant inconsistencies regarding the dates on which the TSC received direction to modify the watchlist statuses, the numbers of individuals for whom statuses were modified, and the dates on which the modifications were made.

For example, in the February 17, 2010, electronic communication, the TSC reported that on December 31, 2009, it identified [REDACTED] persons in the TSDB who met the threat-based criteria for watchlist status modification. Of the [REDACTED], the TSC reported that it upgraded [REDACTED] persons to the Selectee List. However, in the NDIU's October 2010 electronic communication, the TSC reported that it upgraded approximately [REDACTED] persons to the Selectee List.

Further, the February 17, 2010, electronic communication contains limited information regarding the direction for the upgrades for [REDACTED], as well as the date the instructions were provided to the TSC. In that communication, the TSC reported that this request affected the watchlist status of [REDACTED]. However, in the October and December 2010 electronic communications, the TSC reported that it had modified the watchlist status of [REDACTED].

When we discussed these discrepancies with the TSC at our audit close-out meeting and in subsequent communication, officials indicated that the electronic communications were intended to be iterative in nature, representing a snapshot of the populations impacted by the actions. The TSC provided explanations that helped to account for the discrepancies in the numbers of individuals impacted in the two examples cited above. Although the TSC's explanations accounted for the differences and provided the necessary connections between its iterations of the events, the explanations did not address why those connections were not previously documented in its accounts. We believe that the TSC should have done a better job explaining in its electronic communications at the time how the numbers related to each other and how they evolved as tasks were completed, as well as formally documenting all directions received and actions taken.

We discussed this issue with a TSC official who acknowledged the difficulty in maintaining the necessary documentation during crisis situations. The official also said that he believed that the FBI had the necessary procedures in place to ensure major events are properly documented and recalled the difficulties doing so while working in an FBI field division when the terrorist attacks of September 11, 2001, occurred. However, the official noted that the December 25, 2009, event was the first major attempted terrorist attack that the TSC experienced as an organization, and TSC personnel were relatively inexperienced and may not have retained documentation for all of its actions. The TSC official said he believed that TSC



personnel now have a greater appreciation for what types of actions need to be documented.

We also discussed this issue with the Director of the TSC who said that the TSC did experience difficulties in managing these bulk, threat-based watchlist modifications. The TSDB does provide the TSC the ability to track, on a record-by-record basis, the date a record was modified, as well as the identity of the user responsible for modifying the record. However, the TSDB did not permit the TSC to easily generate a listing of all of the records modified in response to the incident on December 25, 2009. As a result, the TSC relied on largely manual processes to track the watchlist modifications and deep dive reviews. Further, according to the TSC Director, the TSDB did not contain critical data [REDACTED] to readily identify individuals who met the threat-based criteria.

To help address these weaknesses, the TSC Director said that the TSC modified the TSDB by creating a tagging feature for watchlist identities. The tagging feature allows a user to assign an administratively created tag to a watchlist identity that will allow the user to categorize the identity as necessary. The TSDB reported that it now can create tags in the TSDB that correlate to particular threat-based populations. As such a category of individuals is identified as a potential threat, the watchlist actions can be taken, and the watchlist records tagged. When the threat abates, the watchlist actions can be reversed and the tags removed from the watchlist records. The TSDB now has the ability to track the complete history of which tags were applied to an identity and, therefore, which identities were related to a threat-based initiative.

To further improve the TSDB, the TSC Director said that the TSC is working to develop a new version of the TSDB that will allow the TSC to not only more efficiently identify individuals who meet threat-based criteria, but also to track the resulting watchlist record modifications. This database modification goes beyond the TSDB tagging feature by assisting in the identification of records meeting declared criteria. The TSC Director anticipated that this modification to the TSDB should help the TSC ensure that all watchlist records for future threat-based modifications are tracked, reviewed, and returned to the appropriate watchlist status for each individual once the threat subsides. The TSC anticipated that this information technology solution would be fully implemented in July 2013.

The failed attack on December 25, 2009, was the first major attempted terrorism event for the TSC, and we understand that maintaining documentation may not be the primary focus during a crisis situation. However, because of the inconsistencies in the TSC's documentation regarding the number and types of records modified and the dates the modification occurred, we have concerns about the TSC's ability to ensure that all watchlist records that were modified as a result of the attempted attack were reviewed and returned to the appropriate individualized status. The recent and planned improvements to the TSDB appear to be steps forward, but we believe that the TSC should develop a comprehensive

procedure to ensure that watchlist modifications resulting from emerging threats and other emergency actions are properly and accurately documented.

### **TSC Managerial Continuity and Significant National Security Events**

We believe that it is essential that the TSC maintain operational readiness at all times. We believe that the failed terrorist attack of December 25, 2009, highlighted a potential vulnerability in the U.S. protective response to such an event because it occurred on a national holiday, which fell on a Friday, and at a time when many federal employees take vacation time.

The executive management team was designed to provide the TSC with ample experience and oversight from each of the participating agencies.<sup>62</sup> However, in the immediate aftermath of the failed attack on December 25, 2009, we found that key managers were on leave and that several positions were vacant or occupied by individuals who were relatively new to the TSC. Many of these individuals were available by telephone and e-mail, and evidence exists to document their involvement in the ongoing discussions of the government's response to the unfolding events.

TSC officials said that in the immediate days following the attempted attack, the environment at the TSC was highly energized and hectic. As a result of changes in the watchlist modification directions and the previously described technical issues with TIDE and the TSDB, the TSC's course of action repeatedly changed during this time. Although they believed that the TSC ultimately responded to the crisis correctly, the officials said that the response may not have been as efficient and as organized as it could have been. For example, as discussed above, the TSC also failed to fully document its actions during the immediate days following the attack. It was not until the Administrative Unit Chief, an FBI employee, returned to the TSC several days after the attack that the TSC began to appropriately document the actions that had been taken in the immediate aftermath of the event.

Because the TSC is responsible for ensuring the accuracy and integrity of the watchlist and coordinating the U.S. government's response during encounters with known or suspected terrorists, we believe that the TSC must ensure that its executive management team possesses sufficient historical knowledge and experience to effectively manage any emerging crisis and should identify a core group of positions that must be physically available in some combination at all times.

---

<sup>62</sup> The TSC is administered by the FBI with support from the Departments of Justice, Homeland Security, and State. The Memorandum of Understanding governing the TSC provides that the Director of the TSC will report to the Attorney General through the FBI and requires that the Principal Deputy Director of the TSC be an employee of DHS. The TSC executive management team also includes a Deputy Director for Operations (an FBI employee), and the Deputy Director - Liaison (a State Department employee). In December 2009, the team also included a Chief of Staff (a DHS employee), Chief Counsel (an FBI employee), Administrative Officer (an FBI employee), and Chief Information Officer (an FBI employee).

## **Review of the U.S. Watchlisting System**

Following the failed terrorist attack, the White House directed a review of the U.S. watchlisting system and the performance of the intelligence, homeland security, and law enforcement communities related to the attempted bombing. The investigation revealed that the federal government possessed all of the information necessary to place the subject on the consolidated terrorist watchlist and prevent him from flying to the United States. However, personnel did not search all available databases and failed to identify, correlate, and fuse into a coherent account all of the discrete, fragmented pieces of information. As a result, NCTC did not provide the TSC with information to watchlist the individual who had committed the failed attack and the TSC was not aware of the individual or involved in any actions related to him until after the event.

In its January 7, 2010, memorandum, the White House directed the TSC to develop recommendations on whether adjustments should be made to the watchlisting nomination criteria, including the biographic and derogatory criteria for inclusion in TIDE, the TSDB, and the No Fly and Selectee Lists. In addition, the TSC was directed to conduct a thorough review of the TSDB and determine the current visa status of all known or suspected terrorists, beginning with individuals on the No Fly List.

According to TSC officials, they met numerous times with representatives from the CIA, the Office of the Director of National Intelligence (ODNI), the National Security Agency (NSA), the NCTC, and the Departments of Justice, Defense, State, Treasury, and Homeland Security. These representatives reviewed the then current watchlisting protocol to determine what changes were needed.<sup>63</sup> According to TSC officials, the revised Watchlist Guidance was approved by an interagency process on May 25, 2010. Following a multi-agency classification review and minor revisions, the final Watchlist Guidance containing these revisions to the watchlisting protocol was issued in July 2010.<sup>64</sup>

## **Conclusion**

Following the failed attempted airline bombing on December 25, 2009, the TSC was verbally directed, through an interagency process, to make temporary watchlist status modifications for certain categories of individuals based on emerging threat information. However, the then-existing watchlist guidance did not address such immediate, threat-based status changes for whole categories of individuals. In some instances, the TSC was directed to include individuals on the watchlist for whom the U.S. government did not possess sufficient information to support inclusion on the watchlist based on pre-existing criteria, but that

---

<sup>63</sup> Protocol Regarding Terrorist Nominations, February 2009.

<sup>64</sup> As noted previously, the Watchlist Community issued new Watchlist Guidance in March 2013, but because the policy document was issued outside the scope of this audit, we did not address it in this report.



government officials believed necessary due to the threat reporting received at that time.

Although the threat-based watchlist modifications were not covered by the then-existing watchlist protocol, the initial directions were not provided or confirmed in writing. As a result, we found that there was the potential for confusion regarding the specific directions provided. In addition, the lack of written direction left the TSC vulnerable to challenges from individuals who believed they were unjustly included on the watchlist.

Further, throughout the successive modification initiatives, we found that the TSC experienced operational, technical, and administrative issues. As a result, in the immediate aftermath of the attempted attack, certain downstream screening agencies did not possess critical terrorist watchlist information about individuals who might pose a potential threat to national security. In addition, because some of the modifications did not conform to the then-existing policy, the TSC was forced to bypass its normal procedures to distribute the information to downstream screening agencies.

Although the TSC confirmed in writing the directions it had been provided regarding watchlist modifications, we also found that the TSC did not adequately document its actions regarding the modifications in the early days following the failed terrorist attack. As a result, the TSC struggled to reconstruct its actions and was unable to provide us with a complete listing of all the records that were modified during the earliest days following the failed terrorist attack.

Finally, in the immediate aftermath of the attempted attack, we found that several positions were vacant or occupied by individuals who were relatively new to the TSC and that, although key TSC managers were available by phone and e-mail, they were not physically present at the TSC. We believe that a lack of sufficient numbers of executives with historical knowledge and experience at the TSC likely contributed to some of the issues we identified.

## **Recommendations**

We recommend that the FBI:

1. Require the TSC to develop formal and comprehensive procedures for the full documentation of crisis events that may result in expedited watchlist upgrades or other emergency actions related to the watchlist. The procedures should address the types of documentation that must be retained, the method of retention, the length of time the documents must be retained, and the individuals responsible for collecting and maintaining the documentation.
2. Require the TSC to continue the development and implementation of enhancements to the TSDB that will allow the TSC to more efficiently identify individuals who meet threat-based criteria and to track any

resulting watchlist record modifications, and also to ensure that modified records are subsequently reviewed in a timely fashion to determine their appropriate watchlist status after the specific threat has passed or the designated period of modification has expired.



## II. FBI WATCHLIST NOMINATIONS AND REMOVALS

During our previous audits of the FBI's watchlist processes, we found that the FBI failed to nominate to the watchlist subjects of terrorism investigations, completed nominations to the watchlist in an untimely manner, and failed to remove subjects of closed terrorism investigations from the watchlist. Generally, we found in this review that the improvements implemented by the FBI as a result of our previous audits have helped to ensure that the watchlist is more complete, accurate, and current. Despite these improvements, we found that the FBI's December 2010 watchlist policy provided a more restrictive set of criteria for inclusion in TIDE and TSDB than outlined by the Watchlist Community.<sup>65</sup> As a result, FBI case agents were not submitting certain terrorism information to NCTC and the TSC for inclusion in TIDE and the TSDB. Therefore, information about known or suspected terrorists may not have been available to the Watchlist Community for analysis and for possible inclusion on the watchlist. In addition, we found that the improvements implemented by the FBI did not ensure that all subjects of FBI investigations were nominated to the TSDB when the investigation is open or are removed from the watchlist when the investigation is closed. We also found that the FBI maintained redundant and inefficient processes which hampered its ability to process watchlist actions in a more timely manner, and the FBI could further refine its policies by tightening its requirement for case agents to submit nomination and removal actions.

### Background

Because of the vital role the consolidated watchlist plays in the detection and apprehension of known or suspected terrorists, it is essential that all subjects of FBI investigations be nominated to the watchlist as quickly as possible. Similarly, individuals should be removed promptly from the watchlist when the government no longer has a reasonable suspicion that the person is a known or suspected terrorist. Leaving individuals on the watchlist longer than necessary increases the chances that these individuals will be stopped or detained during an encounter. In addition, retaining these obsolete records can make it more difficult to accurately identify positive matches to known or suspected terrorists because of similarities in certain peoples' identifying information. Further, retaining individuals on the watchlist needlessly increases the size of the watchlist and wastes resources required to maintain and search it.

---

<sup>65</sup> The FBI Counterterrorism Division (CTD) issued updated watchlist policy guidance in March 2012. We discuss that policy later in this finding.

In our last two reviews, we identified significant weaknesses with the FBI's management of the terrorist watchlist. We made 22 recommendations to the FBI to help ensure that the FBI's watchlist actions were accurate, complete, and timely.

As part of this review, we evaluated whether the FBI's new processes helped to ensure that subjects of FBI investigations were nominated to and removed from the consolidated terrorist watchlist in compliance with FBI policy. Generally, we found that the improvements implemented by the FBI as a result of our previous audits had helped to ensure that the watchlist was more complete and accurate, and nominations from field divisions were submitted in a more timely manner. However, we also identified areas in which we believe the FBI can improve further its processing of watchlist nominations and removals.

In this finding, we first discuss the initiatives implemented by the FBI as a result of our previous audits. Then we assess the impact of these initiatives on the FBI's watchlist nominations for subjects of its preliminary and full terrorism investigations. We conclude this finding with our analysis of the FBI's efforts to remove subjects of closed terrorism investigations from the watchlist.

### **Recent FBI Watchlist Initiatives**

The FBI reported that it had taken a series of corrective actions in response to the recommendations contained in our prior audits.<sup>66</sup> Below, we provide an overview of each initiative and then discuss the initiative's impact on FBI operations.

#### ***FBI Watchlist Guidance***

Following our previous audits, DOJ and the FBI conducted a review of their watchlisting policies and procedures to improve their processing of watchlist actions. During its review, the FBI reported that it found it had issued over 40 electronic communications addressing watchlisting during a 5-year time span. The FBI reported that this large volume of sometimes conflicting policies contributed to employee confusion regarding watchlist procedures. The FBI consolidated its existing guidance and in December 2009 issued a single policy document governing watchlisting.

The FBI's internal guidance provides more comprehensive instructions regarding criteria for inclusion on the watchlist of known and suspected terrorists who are the subjects of FBI investigations. In addition, the guidance outlines the

---

<sup>66</sup> The Office of Management and Budget (OMB) and DOJ have issued policies and procedures for following-up on recommendations of audit reports. These policies are intended to ensure the prompt and proper resolution and implementation of audit recommendations. During this process, the OIG elicits responses from components regarding planned corrective actions. When received by the OIG, the responses are reviewed to determine whether the planned corrective actions meet the intent of the recommendations. When appropriate, the OIG performs subsequent audit work to assess the implementation of certain actions, as we have done in this instance.

conditions under which the FBI may retain individuals on the watchlist for whom the FBI does not have an active investigation, referred to as "non-investigative subjects." The guidance also provides FBI case agents with specific procedures for nominating subjects to the watchlist, modifying existing watchlist records, and removing subjects from the watchlist, including submission and processing timeframes. Further, the FBI included performance metrics for the submission and processing of watchlist actions by its field divisions and headquarters personnel.

Following the failed terrorist attack on December 25, 2009, the FBI reissued its internal watchlist policy to incorporate the modifications made in the TSC's watchlist guidance. Issued in December 2010, the new FBI policy provided guidance on the changes to the reasonable suspicion standard, including a description of particular activities that a nominator should consider in determining whether there is a reasonable suspicion that a person is a known or suspected terrorist. In addition, the FBI's internal guidance was updated to include the new criteria for the No Fly List.

#### *FBI Metrics and Compliance Process*

In April 2009, the FBI implemented a new process to monitor its performance related to watchlist actions, including ensuring that subjects of FBI investigations are appropriately watchlisted. The FBI created within TREX a new Metrics Team that is responsible for tracking FBI field division and headquarters compliance with FBI watchlist policies, including the newly established timeframes for processing watchlist actions.

On the first workday of each month, the Metrics Team runs a report of all preliminary and full international and domestic terrorist investigations that were opened or closed by the FBI during the prior month. The Metrics Team reviews the report to identify the watchlist actions required for terrorism investigations opened or closed during the past month. For example, the opening of new international terrorism investigations should cause the field division to submit a watchlist nomination form to TREX, and the closing of such a matter should trigger a request to remove the corresponding watchlist record.

The TREX Metrics Team then manually compares the case opening and closing information against watchlist actions submitted by the field divisions. Through this comparison, the Metrics Team attempts to identify open or closed terrorism investigations that lack a corresponding nomination or removal package. When the Metrics Team analyst identifies an FBI terrorism case for which the nomination or removal package has not been submitted, the analyst contacts the case agent and requests that the appropriate package be submitted.

The Metrics Team also compiles the data and calculates the amount of time taken by both the field division and TREX to process nomination and removal watchlist actions. The information is compiled in spreadsheets and consolidated



into monthly reports that are distributed to the field divisions and FBI headquarters management for review.

#### *New Database*

In June 2011, the FBI implemented a new database, entitled the Known or Suspected Terrorist (KST) Watchlisting Database. This new database replaced the FBI's existing electronic processes for submitting watchlisting actions. According to TREX, the new KST Database allows case agents to prepare and track watchlist nomination forms and this should make those actions more efficient. Case agents should enter information into a specially formatted document template and once the document is submitted, the information is automatically entered directly into the database and is available electronically for TREX's use. As a result, TREX staff believe that the new database should help to reduce the need for manual data entry and the associated data entry errors, as well as improve the timeliness with which the FBI submits and processes watchlist actions.<sup>67</sup>

#### *TREX Reorganization*

In July 2009, the FBI reorganized TREX to help streamline its processing of watchlist actions.<sup>68</sup> Under the new structure, requests from the field for watchlist actions are submitted electronically to a centralized repository at TREX where they are segregated according to the type of action – nomination, modification and removal, or non-investigative subject. Watchlist actions are then processed by a team of specialized analysts. TREX now has one team that is responsible for processing all FBI watchlist nominations and another team responsible for processing all FBI watchlist modifications and removals. In February 2010, the FBI also formed a new team within TREX, the Non-Investigative Subject Team, to manage and monitor watchlist records related to non-investigative subjects.

Near the end of our audit, the FBI reorganized its Counterterrorism Division (CTD). On March 5, 2012, the FBI transferred TREX from CTD's National Threat Center Section to the TSC.<sup>69</sup> According to FBI documents, the FBI anticipates that this consolidation of TREX within the TSC will help to streamline FBI

---

<sup>67</sup> The FBI is implementing a new case management system. Later in this finding, we briefly discuss the FBI's case management system, as well as the FBI's future plans for the system as it relates to watchlisting.

<sup>68</sup> During our previous reviews, when TREX received a watchlist nomination, modification, or removal form from an FBI field division, that request was forwarded to the employee responsible for that specific field division. We found that assigning work to TREX staff by field division contributed to the FBI's untimely processing of watchlist actions when staff were unexpectedly absent. As a result of our review, TREX modified its processes and organizational structure as described above.

<sup>69</sup> The FBI's National Threat Center Section is housed within the CTD. The section is the focal point for all incoming threat information, including the preliminary analysis of emerging international and domestic terrorism threats and assignment for immediate action within the FBI.

watchlist nominations by eliminating review functions that previously were duplicated.

### **FBI Watchlist Nominations**

When an FBI field division opens a preliminary or full terrorism investigation, FBI policy requires that FBI headquarters be notified within 10 business days of the initiation of the investigation. To accomplish this, the case agent prepares an electronic communication that is submitted for supervisory approval. Once the field division supervisor approves the opening of the case, the electronic communication is uploaded into the FBI's automated case management system (which formally opens the case within the FBI). FBI policy requires that the electronic communication in a terrorism matter contain an "action lead" or an electronic prompt that notifies FBI headquarters of the case opening. FBI policy also requires that the field division include in the electronic communication an action lead to TREX requesting that the subject be entered in all appropriate government watchlists.

To assess whether the FBI's new metrics and compliance processes helped to ensure that subjects of FBI investigations were nominated to the consolidated terrorist watchlist in compliance with FBI policy, we reviewed FBI TREX Metrics Team and corresponding watchlist data. We reviewed Metrics Team and watchlist data for 115 subjects of preliminary and full domestic or international terrorism cases *opened* during the first quarter of FY 2011 in four FBI field divisions: Chicago, Illinois; Los Angeles, California; Miami, Florida; and Minneapolis, Minnesota.<sup>70</sup> In addition, to assess the impact of the FBI's new KST Database, we reviewed nomination data for watchlist actions processed using the new database.<sup>71</sup> Specifically, we reviewed nomination data for 120 subjects of preliminary and full domestic or international terrorism cases *opened* during the fourth quarter of FY 2011 pertaining to the aforementioned four FBI field divisions.

Generally, we found that the improvements implemented by the FBI as a result of our previous audits helped to ensure that the watchlist is more complete, accurate, and current. Despite these significant improvements, however, we identified areas in which we believe the FBI has opportunities to improve its processing of watchlist nominations.

### ***Subjects Not Watchlisted***

In our previous audit, we found that the FBI had not consistently nominated known or suspected terrorists to the consolidated terrorist watchlist in accordance

---

<sup>70</sup> There were 113 cases opened in these four field division locations during the first quarter of FY 2011. However, one case had multiple associated subjects. Appendix I contains additional information about our audit scope and testing methodology.

<sup>71</sup> Because the FBI implemented its new KST Database in June 2011, we tested watchlist data for the fourth quarter of FY 2011 and compared the results to the FBI's prior performance.



with FBI policy.<sup>72</sup> During our current review, we found that the FBI's metrics and compliance process helped to significantly reduce the number of subjects of FBI cases that were not nominated to the watchlist. Compared to our previous audit in which 15 percent of the subjects of the cases we reviewed were not nominated to the watchlist, during our review of 115 subjects in our sample of investigations opened during the first quarter of FY 2011, we did not identify any subjects who were not nominated to the watchlist as required by FBI policy.

However, we still found subjects of cases opened prior to the first quarter of FY 2011 who had not been nominated to the watchlist. During our review of the Metrics Team's analysis of actions taken on 1,018 cases closed during January 2009 through December 2010 in the four field divisions in our sample, we found that the Metrics Team's monthly results indicated that a total of 19 subjects (nearly 2 percent) had not been nominated to the watchlist while the case was open. Further, during our review of non-investigative subjects, we found an additional four subjects of investigations that closed during 2010 who had not been nominated to the watchlist while the case was open.<sup>73</sup> When these four subjects were nominated to the watchlist later in 2010, they were all nominated to the No Fly List.

We asked the Metrics Team Leader how this may have occurred. She indicated that an individual who is an appropriate candidate for the watchlist may be identified at the opening of an investigation, but the case agent may not yet possess sufficient identifying information to permit watchlisting. [REDACTED]

[REDACTED]. Once the case agent obtains sufficient biographical information, the case agent may forget to submit the appropriate paperwork to have the individual watchlisted. The FBI reported that its supervisors are required to conduct regular case file reviews with case agents to help ensure the subjects are appropriately watchlisted. However, despite these supervisory reviews, the subjects we identified still were not nominated to the watchlist while the case was open.

According to the FBI's December 2009 and December 2010, watchlist policies, case agents were directed to submit a watchlist nomination package for subjects of both preliminary and full domestic and international terrorism

---

<sup>72</sup> During our review in May 2009, we reviewed a total of 216 cases that were initiated or closed during FY 2006, FY 2007, and the first half of FY 2008 in the following field divisions: Los Angeles, Miami, and Minneapolis.

<sup>73</sup> These 4 were included within 49 requests for the watchlisting of non-investigative subjects that we reviewed for cases closed after December 7, 2009, and processed by the FBI during the period of January 2010 to December 2010. The watchlisting of non-investigative subjects, including the timeliness of such actions, is discussed in detail in Finding III below, and these four nominations are specifically identified in Exhibit 4-1.

investigations.<sup>74</sup> Yet, later in the same policy, case agents were instructed that they were to submit the watchlist nominations only once the case agent possessed sufficient identifying information – [REDACTED]. If there was insufficient identifying information when the investigation was first opened, then the case agent was required to submit the watchlist nomination once the subject's information was obtained at a later date.

During our examination of documents regarding the Watchlist Community's review of watchlisting practices following the attempted terrorist attack on December 25, 2009, and the resulting revision of the Watchlist Guidance, we noted that there were substantial discussions about the amount of biographical information needed for watchlisting and the sharing of intelligence information within the Watchlist Community. Specifically, these discussions included the expression of concerns that some agencies were only nominating individuals for whom the U.S. government possessed [REDACTED]. In response, the Watchlist Community directed several agencies to review their historical data to determine if individuals not previously watchlisted should be nominated to the watchlist. The FBI was not one of the agencies directed to review its historical practices.

We asked the TSC Director and Chief Counsel about the FBI's policy and the Watchlist Community concerns about the inconsistency in the threshold for identifying information required for nominations. The TSC Director and Chief Counsel agreed that the FBI's December 2009 and December 2010 policies appeared to restrict the FBI's watchlist nominations, as well as the amount of terrorism information shared with NCTC. These officials said they believed that, in cases where the FBI has a reasonable suspicion to believe the subject is a known or suspected terrorist, the FBI should be forwarding all identifying information to NCTC for analysis and possible watchlisting, even when only partial biographical identifiers are available.

The TSC Director said he believed that sending all FBI terrorism information to NCTC and TSC provided the opportunity for terrorism information to be integrated and augmented and may help to further reduce the number of subjects of FBI investigations who are not watchlisted. The TSC Director said that once the FBI submits the terrorism information to NCTC and the TSC, the information would be available for analysis by the Watchlist Community. Other members of the Watchlist Community might possess additional biographical information about the FBI subject that, when combined with the FBI's information, would provide sufficient information for watchlisting.

We reviewed the FBI's nomination practices in instances where FBI terrorism cases had been opened on [REDACTED]. Of the 115

---

<sup>74</sup> The FBI's policies on investigative activity and related watchlist nominations are discussed in detail in the Introduction section of our report under the heading "Overview of Internal FBI Watchlist Processes." As discussed, FBI policy permits the exclusion from the watchlist of subjects of full domestic terrorism investigations that focus on groups or organizations that are involved in national security threats to the public.

subjects in our sample of investigations opened during the first quarter of FY 2011 in four field offices, we identified 39 subjects for whom the field office opened a terrorism investigation when they did not possess [REDACTED]. As shown in Exhibit 3-1, of the 39 subjects lacking [REDACTED], we found that for 8 of these subjects the FBI possessed a [REDACTED] at the time the case was opened, thus meeting the identifying information standard for the TSDB. Five of the subjects with [REDACTED] were the subject of a full investigation and, therefore, would also necessarily meet the reasonable suspicion standard for watchlisting. However, the field division submitted a watchlist nomination package for just one of these eight subjects.

**Exhibit 3-1**  
**Sample FBI Cases with Subject Information**  
**Less than [REDACTED]**  
**by Investigation Type**

	Preliminary Investigation	Full Investigation	Total
[REDACTED] only	2	4	6
[REDACTED] only	1	0	1
[REDACTED] only	0	1	1
<b>Total</b>	<b>3</b>	<b>5</b>	<b>8</b>

Source: OIG analysis of FBI data

For the one subject for whom the field office did submit a watchlist nomination, the case agent possessed only the subject's [REDACTED]. According to the Metrics Team Leader, the case agent initially did not submit a watchlist nomination package at the time the case was first opened. Upon further searches of TIDE, the case agent found that the [REDACTED] matched other fragmentary information for an individual already included in TIDE. The case agent identified this information in TIDE more than 2 months after the opening of the investigation and thereafter submitted the nomination.

In August 2011, we discussed the results of our analysis with FBI CTD officials and expressed our concern that the FBI's December 2010 policy was inconsistent with the Watchlist Community Guidance, thereby unduly restricting the FBI's sharing of information with NCTC and the FBI's nominations to the watchlist.<sup>75</sup>

Despite the results of our review, the FBI CTD officials said that they believed that the FBI's December 2010 policy was sufficient. That policy indicated that case agents should submit nominations to TREX for all subjects of preliminary and full terrorism investigations, so that TREX can evaluate whether the reasonable suspicion standard had been met for watchlisting. FBI CTD officials stated that they believed this worked well. These officials said that TREX was best qualified to

<sup>75</sup> For inclusion in TIDE, NCTC requires that the nominating agency provide evidence of a nexus to terrorism. However, regarding necessary identifying information, NCTC accepts fragmentary information without names, [REDACTED].

review the nomination and assess whether the subject warranted watchlisting in accordance with FBI policy. We acknowledge that such a process flow could work well if the policy was sufficiently clear, and FBI personnel were forwarding nominations for the subjects of all terrorism investigations. However, the results presented in Exhibit 3-1 above are from cases opened in the first quarter of FY 2011 and this aspect of the FBI's policy had been stated in the same way since at least December 2009. These results indicate that FBI personnel are not, in fact, submitting nominations in all instances. As a result, information on the subjects may not have been available to the Watchlist Community for analysis and possible watchlisting.

Following our discussions with FBI CTD and TSC officials, the FBI revised its watchlisting nomination guidelines in March 2012 to be more consistent with the minimum identifying criteria set forth in the July 2010 Watchlisting Guidance. For example, the FBI's nomination policy now has a distinct section that outlines the identifying criteria that is required for watchlisting, namely the subject's last name and at least one additional identifier (e.g., first name, [REDACTED], passport [REDACTED]). In addition, FBI personnel are informed that if they do not have one of the specifically named additional identifiers, watchlist nominations are required when two or more of certain additional identifiers are known (e.g., [REDACTED]).

Although the FBI's March 2012 policy now reflects the minimum identifying criteria set forth in the July 2010 Watchlisting Guidance, the policy still includes the following: [REDACTED]

[REDACTED]. The FBI should review its policy document to ensure that the multiple sections on watchlist nominations are internally consistent and work with the TSC to ensure that the policies are in line with the requirements of the Watchlist Community.

In addition, the FBI did not indicate whether it intended to review terrorism investigations opened under the previous policy guidelines to ensure that the individuals that meet the current criteria are now appropriately watchlisted. Therefore, we recommend that the FBI review the subjects of terrorism investigations opened under its previous policy guidelines to determine whether the FBI possesses sufficient biographical and derogatory information under the revised policy to support forwarding the information to NCTC for review and potential watchlisting.

#### *Timeliness of Watchlist Nominations*

Following our previous audit examining the timeliness of the FBI's watchlist nominations, the FBI revised its time requirements as outlined in its policy



document dated December 2009.<sup>76</sup> As shown in Exhibit 3-2, when it implemented its December 2009 watchlist guidelines, the FBI retained the existing requirement for its field divisions to submit non-expedited watchlist nominations to TREX within 10 business days of the date the case is opened in the FBI's case management system.<sup>77</sup> For TREX, the FBI increased the amount of time allocated for processing watchlist nominations.

<b>Exhibit 3-2</b>		
<b>FBI Watchlisting Compliance Timeline – Nominations</b>		
	<b>Field Division</b>	<b>TREX</b>
<b>Prior</b>	10 business days from date case is opened in case management system.	24 hours from receipt of complete package from field division.
<b>New</b>	10 business days from date case is opened in case management system.	5 business days from receipt of complete package from field division.

Source: Federal Bureau of Investigation

Prior to December 2009, TREX's goal was to complete its processing of watchlist nominations within 24 hours of receiving a complete package from the field.<sup>78</sup> Under the 2009 and subsequent guidelines, TREX is now required to complete its processing of watchlist nominations within 5 business days of receiving a complete package from the field. The FBI attributed the need to increase the processing time for TREX to the expanded role that TREX now has in independently verifying the accuracy of each identifier on the nomination form and searching relevant databases for additional identifiers.<sup>79</sup>

Based on our review of TREX Metrics Team and watchlist nomination data, we found that overall the FBI has significantly improved its compliance with FBI

<sup>76</sup> The FBI has since issued new policy in December 2010 and March 2012. These new policies did not change the timeliness guidelines first established in December 2009.

<sup>77</sup> The only exception to this 10-business day rule is when the terrorism subject is being nominated to the TSA's No Fly List. In these cases, FBI policy requires that these subjects be nominated to the watchlist by the field divisions within 24 hours, and TREX must then process the nomination within 24 hours of receipt. The TSA's No Fly List includes names of individuals who will be denied transport on commercial flights because they are deemed a threat to civil aviation, U.S. facilities, or U.S. vessels. Following the attempted terrorist attack on December 25, 2009, the President directed that a review of the No Fly and Selectee List criteria be conducted. The committees that conducted the review recommended changes to the criteria and implementation guidance. Those recommendations were approved by the interagency working group on May 25, 2010.

<sup>78</sup> According to the FBI, at the time of our previous audit, TREX's responsibilities were more limited and analysts entered the subject's information into the FBI's National Crime Information Center (NCIC) and then forwarded the nomination package to the NCTC.

<sup>79</sup> We discuss the appropriateness of this change in timeliness requirement in the following section.



policy for nominations to the watchlist.<sup>80</sup> As shown in Exhibit 3-3, the FBI considerably reduced the number of untimely watchlist nominations from the 78 percent identified in our May 2009 audit to 14 percent for the first quarter of FY 2011.<sup>81</sup> Further, the metrics and compliance process has helped to ensure that unwatchlisted subjects are identified sooner and placed on the watchlist. During our previous audit, we found that the maximum amount of time taken by the FBI to nominate a subject to the watchlist was 307 days. With the metrics and compliance process, the FBI reduced the maximum amount of time to just 15 days. Moreover, the FBI has reduced the average number of days that elapse between case opening and watchlisting from 42 days to 5 days. Similarly, the FBI has reduced the median number of days that elapse from 29 days to just 4 days.

---

<sup>80</sup> We identified some data entry errors in the Metrics Team calculations. However, the errors were minor and did not significantly impact the Metrics Team's results.

<sup>81</sup> For purposes of our testing, we assessed TREX for processing watchlist nominations within 5 business days of receipt of a complete watchlist package. We considered a subject to be untimely nominated if either the field division or TREX exceeded its standard processing time. For example, if a field division submitted a nomination within 12 business days and TREX processed the nomination within 1 working day, we considered such a nomination untimely because the field division did not meet the timeliness standard.

**EXHIBIT 3-3**  
**Untimely Watchlist Nominations<sup>82</sup>**

	OIG Audit May 2009 <sup>83</sup>	1 <sup>st</sup> Quarter FY 2011 (Before KST Database Implementation) <sup>84</sup>	4 <sup>th</sup> Quarter FY 2011 (After KST Database Implementation) <sup>85</sup>
Number Tested	95	76	92
Number Untimely	74	11	17
Percent Untimely	78%	14%	18%
Minimum in Days	4	1	1
Maximum in Days	307	15	63
Average in Days	42	5	19
Median in Days	29	4	11

Source: OIG analysis of FBI data

During the Implementation of the KST Database in the fourth quarter of FY 2011, the FBI and TREX experienced an increase from 14 percent to 18 percent in untimely nominations. We attribute some of the untimely nominations to normal reductions in productivity when new systems are implemented. In that regard, we found that, as the FBI gained familiarity with the new KST Database, the number of untimely nominations was lower in each month of the fourth quarter of FY 2011.

During the implementation of the KST Database, we anticipated relatively small increases in processing days. However, we noted that the maximum number of days that a subject was not watchlisted more than quadrupled from the first to the fourth quarter of FY 2011, and the average and median number almost quadrupled and tripled, respectively. According to the Metrics Team data, this was attributable to case agents continuing to forget to submit the nominations in a timely fashion.

<sup>82</sup> To examine the 10-business day requirement for field divisions, we used the date the case was opened in the FBI's case management system and compared it to the date TREX received a complete nomination package from the field division. To examine the 5-business day requirement for TREX, we used the date TREX received the complete package from the field and the date TREX forwarded the nomination to the NCTC branch staffed by FBI personnel.

<sup>83</sup> During our review in May 2009, we reviewed the timeliness of FBI watchlist nominations for 95 cases that were opened during FY 2006, FY 2007, and the first half of FY 2008. The field divisions included Los Angeles, California; Miami, Florida; and Minneapolis, Minnesota.

<sup>84</sup> There were 115 subjects of cases opened during the first quarter of FY 2011. During our review of the nominations for the subjects in our sample cases, we identified 39 subjects who did not meet the FBI's existing criteria for watchlisting. Therefore, we excluded these 39 subjects from our testing for timeliness.

<sup>85</sup> There were 120 subjects of opened cases in the four field divisions in our sample during the fourth quarter of FY 2011. During our review of the nominations for the subjects in our sample cases, we identified 28 subjects of terrorism cases who did not meet the FBI's existing criteria for watchlisting. Therefore, we excluded these 28 subjects from our testing for timeliness.

Although the FBI has significantly improved its overall compliance with existing time requirements, we believe that the FBI would benefit from further refining its processes and timeliness standards. The following sections discuss specific areas of improvement that we believe should be considered for the field divisions and TREX.

### Field Divisions

Although the FBI field divisions have improved their compliance with existing timeframes, we believe that the timeframe permitted under FBI policy for the submission of watchlist nominations is unnecessarily long. Once a case agent receives supervisory approval to open a terrorism case, the case agent has 10 business days to submit a watchlist nomination. With TREX's additional 5 business days to process the watchlist nomination, it could take up to 15 business days from the date the FBI first becomes aware of an individual to the time the individual is submitted to NCTC or TSC for watchlisting. With 2 additional days allocated for NCTC and TSC review, the FBI's current guidelines allow up to 17 business days – or potentially more than 3 weeks – to elapse before a potential threat is nominated to the watchlist.<sup>86</sup>

Based on our analysis of FBI watchlist data, we believe that the timeliness guidelines for the field divisions could easily be shortened. As shown in Exhibit 3-4, we found that the field divisions normally submit watchlist nominations in advance of the 10-business day requirement. The field divisions in our sample submitted approximately two-thirds of the watchlist nominations within 2 business days of opening the investigation in the automated case management system, and 80 percent of the nominations within 5 business days.

**EXHIBIT 3-4**  
**Watchlist Nominations Submitted by**  
**FBI Field Divisions**

Time Elapsed from Case Open to Nomination	Percentage of Nominations		
	OIG Audit May 2009	1 <sup>st</sup> Quarter FY 2011 (Before KST Database Implementation)	4 <sup>th</sup> Quarter FY 2011 (After KST Database Implementation)
1 day or less	19%	62%	51%
2 days or less	23%	72%	66%
3 days or less	28%	80%	70%
4 days or less	31%	86%	79%
5 days or less	34%	87%	80%
10 days or less	53%	89%	87%
>10 days	47%	11%	13%

Source: OIG analysis of FBI watchlist data

<sup>86</sup> For example, if the case agent received supervisory approval to open a terrorism investigation on Tuesday, May 7, 2013, an eligible subject might not be included on the watchlist until 24 days later, on Friday, May 31, 2013, and still be considered a timely nomination in light of weekends and an intervening holiday.



We discussed the metrics process and processing timeframes for nominations with headquarters and field division officials. These officials said that the metrics process has been a valuable tool for helping the field divisions to submit watchlist nominations in a more timely manner. However, several of the officials said that they believed that some of the watchlist processes could be further streamlined and improved. For example, current FBI policy recommends that preparing and submitting nomination forms at the same time as the case is opened as a "best practice." Several officials said that they believed that the field divisions could readily prepare and submit these forms at the same time as the case is opened.

Also, TREX officials said that the new KST Database should help case agents to prepare and submit watchlist nomination forms in a more timely fashion by eliminating redundant data entry. The new database incorporates a specially formatted form to generate the case opening electronic communication. When the case agent prepares the opening electronic communication, the information from the opening electronic communication automatically populates the watchlist nomination form. Therefore, the new database should further shorten the time to prepare the nomination form because the case agent enters case information only once.

In our May 2009 report, we recommended to the FBI that it evaluate the overall watchlisting process to determine the total amount of time that is reasonable and necessary to ensure a timely but thorough watchlisting process. In its April 24, 2009, response to this recommendation, the FBI stated that it had conducted such an evaluation. At that time, the FBI reported that it believed field divisions should submit non-expedited nomination packages to TREX within 2 days of receiving supervisory approval to open the case.

The final guidance issued by the FBI in December 2009 did not direct the field division to submit non-expedited nominations to TREX within 2 business days. Rather, the FBI maintained its original 10-business day timeframe for submitting watchlist nominations. The FBI did not provide an explanation for continuing its 10-business day timeframe. In correspondence subsequent to our audit, the FBI reported that its timeframe for submitting watchlist nominations would remain unchanged until sustained improvement in nominations was achieved. The FBI indicated that once sustained improvement had been achieved, it would re-evaluate its timeliness requirements.

Although the FBI did not adopt a 2-day nomination standard, in the first quarter of FY 2011 the field divisions in our sample were already submitting nearly three-fourths of the watchlist nominations within 2 business days of case openings, and nearly two-thirds within this time frame during the fourth quarter of FY 2011 (even with a new system).

In our opinion, retaining the existing 10-business day timeframe increases the potential risk that nominations may not be processed with a sufficient sense of urgency. By contrast, reducing this time standard would be a strong indication to

the field divisions that it is important to accomplish this essential national security task in an expeditious manner. Therefore, we recommend that the FBI re-assess its timeframe for field division watchlist nominations and also consider mandating as a requirement its current "best practice" that "nominations will be submitted at the same time as the opening communication." Considering the speed at which threats can develop and mature, as evidenced by the events on and immediately following December 25, 2009, we believe that the FBI should identify the means to achieve this "best practice" and mandate expeditious inclusion of eligible persons on the watchlist. We believe that FBI should explore technological solutions within its case management system that would automatically trigger the generation of a watchlist nomination when a case agent officially opens a case and has the requisite identifying information for nomination.

### TREX

The comparison of TREX's current performance for processing watchlist nomination packages to its performance during the period under review in our May 2009 audit is complicated by TREX's expanded role in the nomination processes, as well as the relaxation of its timeliness standards.

As shown in Exhibit 3-5, during the period of review for our May 2009 audit, TREX processed 83 percent of watchlist nomination packages within 5 business days. For the 76 subjects of cases opened during the first quarter of FY 2011, TREX processed 95 percent of the nominations within 5 business days, resulting in a decrease from 17 percent to 5 percent in nominations that took TREX more than 5 days to process.

**EXHIBIT 3-5**  
**Watchlist Nominations Processed by TREX**

Time Elapsed from Case Open to Nomination	Percentage of Nominations		
	OIG Audit May 2009	1 <sup>st</sup> Quarter FY 11 (Before KST Database Implementation)	4 <sup>th</sup> Quarter FY 11 (After KST Database Implementation)
1 day or less	53%	7%	5%
2 days or less	61%	11%	9%
3 days or less	70%	29%	30%
4 days or less	77%	54%	60%
5 days or less	83%	95%	89%
>5 days	17%	5%	11%

Source: OIG analysis of FBI watchlist data

However, the watchlist nomination packages that TREX processed in less than 5 days has significantly declined since our last audit. As previously discussed, at the time of our last audit TREX analysts verified that justification for the nomination existed, reviewed the nomination package for accuracy, verified that the subject met the criteria for inclusion on the watchlist, entered the subject's information into NCIC, and then forwarded the nomination package to the NCTC.



TREX attempted to process both watchlist nominations and removals within 1 business day of receipt. As shown in Exhibit 3-5, TREX met that goal just over half the time, and processed 70 percent of watchlist nominations within 3 business days of receipt. However, during this audit, we found that the percentage of nominations processed within 3 business days of receipt dropped to 29 percent for the first quarter of FY 2011 and 30 percent for the fourth quarter of that fiscal year.

TREX officials attributed this decline in the rapid processing of nominations to TREX's expanded role in independently verifying the accuracy of each identifier on the nomination form and searching relevant databases, including Intelligence Community records, for additional identifiers. In addition, TREX officials explained that TREX had experienced increases in workload resulting from the FBI's policy revision that now requires field divisions to submit watchlist nominations for subjects of nearly all domestic terrorism investigations.<sup>87</sup> Further, TREX officials said that they had experienced staffing shortages during the first quarter of FY 2011 because of extended leave.

To evaluate the impact of these factors on TREX's timeliness, we first discussed TREX's watchlist nomination process with a TREX senior analyst who said that TREX began searching other databases to supplement the information on the watchlist nomination form several years ago. According to the senior analyst, the old FBI nomination form did not contain critical information that could be included with the nomination, such as [REDACTED]. The senior analyst also said that TREX was performing many of the current database searches prior to our May 2009 audit. However, TREX did implement searches of at least two new systems since the last OIG audit.

We expressed our concerns to the FBI that watchlist nominations may have been unnecessarily delayed while TREX analysts searched for additional information that was not critical to placing these individuals on the watchlist. TSC officials informed us that as of December 2012, TREX does not search for the type of additional information discussed above.

To evaluate the impact on workload of the FBI's policy revision that required field divisions to submit watchlist nominations for subjects of nearly all domestic terrorism investigations, we analyzed FBI data on the number of domestic terrorism nominations processed by TREX. As shown in Exhibit 3-6, during the period prior to the implementation of the FBI's new policy, TREX processed an average of [REDACTED] watchlist nominations for known or suspected domestic terrorists per month. During the first 6 months of calendar year (CY) 2010 following the implementation of the FBI's new policy, the FBI had an increase in the domestic terrorism nominations processed by TREX. During this period, TREX processed an

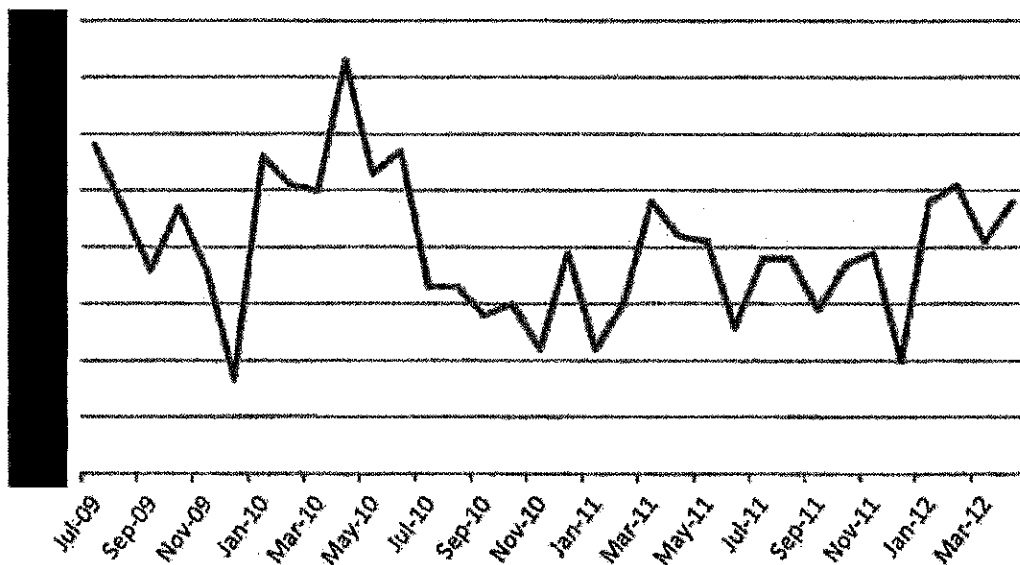
---

<sup>87</sup> As previously discussed in the Introduction, the FBI's previous policy stated that known or suspected domestic terrorists who are subjects of preliminary investigations could be nominated to the watchlist at the discretion of the responsible FBI field division. On December 7, 2009, the FBI revised its policy to require the nomination of subjects of most domestic terrorist investigations, including preliminary investigations.

average of ■ domestic terrorism nominations per month. Following this peak period, TREX processed an average of ■ domestic terrorism nominations per month.<sup>88</sup>

Although TREX experienced an increase in the number of domestic terrorism nominations during the first 6 months following the implementation of the new policy, this time period also coincided with the failed terrorist attack of December 25, 2009. Further, during the second 6 months of CY 2010 following the implementation of the FBI's policy, the number of domestic terrorism nominations processed by TREX had declined to its pre-December 25<sup>th</sup> levels or an average of ■ domestic terrorism nominations per month. Further, we also note that during the first quarter of FY 2011, the period for which we conducted our workload analysis, domestic terrorism nominations accounted for just 15 percent of the nominations processed by TREX.

**EXHIBIT 3-6**  
**Number of Nominations Processed by TREX**  
**for Domestic Terrorism Cases**  
 (July 2009 through April 2012)



Source: OIG analysis of FBI data

We also obtained TREX staffing and workload data. As shown in Exhibit 3-7, when compared to its workload and staffing levels at the time of our prior audit, TREX experienced a net increase of just over 1 percent in its workload during the first quarter of FY 2011. During the same period, TREX experienced a decrease of nearly 10 percent in its actual staffing levels. As a result, TREX staff each

<sup>88</sup> We calculated this average using the 22-month period of July 2010 through April 2012.